FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
08 30 2016
583855
SECRETARY
ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**DOCKET NO. 9357**
	)	
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	

RESPONDENT LabMD, INC.'S APPLICATION FOR STAY OF FINAL ORDER PENDING REVIEW BY A UNITED STATES COURT OF APPEALS

Pursuant to Commission Rule 3.56, 16 C.F.R. § 3.56, Respondent LabMD, Inc. ("LabMD") hereby timely[1] applies to the Federal Trade Commission ("FTC" or "Commission") for a stay of the effective date of its Final Order dated July 28, 2016 in the above-captioned matter, pending judicial review by a United States Court of Appeals.

Patrick J. Massari
Erica L. Marshall
CAUSE OF ACTION INSTITUTE
1875 Eye Street, NW
Suite 800
Washington, DC 20006
Tel. (202) 499-4232
Fax (202) 338-5842
patrick.massari@causeofaction.org

August 30, 2016

Counsel for Respondent LabMD, Inc.

[1] Secretary Clark published the Final Order on July 29, 2016, which was served on LabMD and its Counsel on August 1, 2016, pursuant to Commission Rule 4.4(a)(1)(ii-iii), 16 C.F.R. §§ 4.4(a)(1)(ii-iii).

TABLE OF CONTENTS

TABLE OF CONTENTS……..i

TABLE OF AUTHORITIES……...ii

RECORD REFERENCES AND GLOSSARY……..vii

I. INTRODUCTION……...1

II. BACKGROUND…….....3

III. STANDARD FOR STAY PENDING REVIEW……..…8

A. LIKELIHOOD OF SUCCESS ON APPEAL……....9

1. This Case is Based on A Complex Factual Record and Raises Important Issues…….9

2. LabMD Is Likely to Succeed on Petition for Review……12

i. Commission Erroneously Denied LabMD's Dispositive Motions and Wrongly Rejected LabMD's Jurisdictional and Facial and As-Applied Due Process Arguments……12

ii. The Commission Opinion Misconstrued Section 5's Plain Language……..14

iii. The Commission Opinion is Unsupported By Evidence and Contrary to Law.15

iv. The Commission Opinion Erroneously Ignored Initial Decision's Evaluation of Complaint Counsel's Harm Experts…….19

v. FTC Staff's Relationship with Tiversa Violates Fourth Amendment……...20

vi. Improper Cost-Benefit Analysis……...20

vii. Commission Order is Unlawful and Unenforceable…….21

viii. Unlawful Issuance of Complaint……..24

ix. Commission Part 3 Administrative Process Violates Due Process……...24

B. IRREPARABLE HARM TO RESPONDENT ABSENT STAY…….25

1. Unpayable and Irrecoverable Compliance Costs……..25

2. Violations of Constitutional Rights……..26

3. Reputational Harm……...29

C. HARM TO OTHER PARTIES AND PUBLIC INTEREST……...30

CONCLUSION……..31

[PROPOSED] ORDER GRANTING RESPONDENT LabMD, INC.'S APPLICATION FOR STAY OF FINAL ORDER PENDING REVIEW BY A UNITED STATES COURT OF APPEALS.....32

CERTIFICATE OF SERVICE……...34

CERTIFICATE OF ELECTRONIC FILING…….35

EXHIBITS…….36

TABLE OF AUTHORITIES

CASES

UNITED STATES SUPREME COURT

Armstrong v. Manzo, 380 U.S. 545 (1965) …….....26
Chamber of Commerce v. Whiting, 131 S. Ct. 1968 (2011) ……15
Christensen v. Harris Cnty., 529 U.S. 576 (2000) ……..…15
Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) ……...15
Conn. Nat'l Bank v. Germain, 503 U.S. 249 (1992) ……...15
Connally v. Gen. Constr. Co., 269 U.S. 385 (1926)……14
Credit Suisse Sec. (USA) LLC v. Billing, 551 U.S. 265 (2007)……13
Elrod v. Burns, 427 U.S. 347 (1976) ……..26
FCC v. Fox TV Stations, Inc., 132 S. Ct. 2307 (2012)……13-14, 29
FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120 (2000)……13
FTC v. Cement Institute, 333 U.S. 683 (1948) ……27-28
FTC v. Klesner, 280 U.S. 19 (1929) ……...…24
FTC v. Henry Broch & Co., 368 U.S. 360 (1962) ……..27
FTC v. Ruberoid Co., 343 U.S. 470 (1952) ……23
Giaccio v. Pa., 382 U.S. 399 (1966)……..14, 29
La. Pub. Serv. Com. v. FCC, 476 U.S. 355 (1986) ……13
Mathews v. Eldridge, 424 U.S. 319 (1976) ……26
Schindler Elevator Corp. v. United States ex rel. Kirk, 563 U.S. 401 (2011) ……..…15
Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016) ……...15
Util. Air Regulatory Grp. v. EPA, 134 S. Ct. 2427 (2014) ……..…13
Williams v. Pa., No. 15-5040, 579 U.S. ___, 2016 U.S. LEXIS 3774 (2016)……..25
Withrow v. Larkin, 421 U.S. 35 (1975)……..25

UNITED STATES COURTS OF APPEALS

B&B Insulation v. OSHRC, 583 F.2d 1364 (5th Cir. 1978) ……18
Department of Treasury v. FLRA, 837 F.2d 1163 (D.C. Cir. 1988) …….. 18
Fla. Mach. & Foundry, Inc. v. OSHRC, 693 F.2d 119 (11th Cir. 1982)……..……18
Ford Motor Co. v. FTC, 673 F.2d 1008 (9th Cir. 1981) …….……14
FTC v. Civil Service Training Bureau, Inc., 79 F.2d 113 (6th Cir. 1935) ……...…23
FTC v. World Travel Vacation Brokers, Inc., 861 F.2d 1020 (7th Cir. 1988) ……22

FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) ……..11, 13

Georgia Pac. Corp. v. OSHRC, 25 F.3d 999 (11th Cir. 1994)……..13, 27

Heater v. FTC, 503 F.2d 321 (9th Cir. 1974) …….22

International Dairy Foods Ass'n v. Amestoy, 92 F.3d 67 (2d Cir. 1996)……29

KH Outdoor, LLC v. Trussville, 458 F.3d 1261 (11th Cir. 2006)……30

Knoll Associates, Inc. v. FTC, 397 F.2d 530 (7th Cir. 1968) ……..20

LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015) ……24

LeBlanc v. Unifund CCR Partners, 601 F.3d 1185 (11th Cir. 2010) …….13

Libas, Ltd. v. United States, 193 F.3d 1361 (Fed. Cir. 1999) ……..20

Libbey-Owens-Ford Glass Co. v. FTC, 352 F.2d 415 (6th Cir. 1965 …….22

New Standard Pub. Co. v. FTC, 194 F.2d 181 (4th Cir. 1952) ……...23

Odebrecht Constr. v. Sec'y, Fla. DOT, 715 F.3d 1268 (11th Cir. 2013)……30

Pasha v. Gonzales, 433 F.3d 530 (7th Cir. 2005) …….....19

Rambus, Inc. v. FTC, 522 F.3d 456 (D.C. Cir. 2008)……..16

Rodale Press, Inc. v. FTC, 407 F.2d 1252 (D.C. Cir. 1968) ……...18

Schering-Plough Corp. v. FTC, 402 F.3d 1056 (11th Cir. 2005) …….15-16, 19, 27

S&H Riggers & Erectors, Inc. v. OSHRC, 659 F.2d 1273 (5th Cir. 1981)……...13, 18

Silverpop Sys. v. Leading Mkt. Techs., Inc., No. 14-14258, 2016 U.S. App. LEXIS 196 (11th Cir. Jan. 5, 2016) (unpublished) …….....16-17

Standard Oil Co. v. FTC, 577 F.2d 653 (9th Cir. 1978) ……..22

Trinity Broad. v. FCC, 211 F.3d 618 (D.C. Cir. 2000)……13

Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006) …….24

UNITED STATES DISTRICT COURTS

America's Health Ins. Plans v. Hudgens, 915 F. Supp. 2d 1340 (N.D. Ga. 2012)……...25

Bonnette v. D.C. Court of Appeals, 796 F. Supp. 2d 164 (D.D.C. 2011)……26

Bray v. City of New York, 04 Civ. 8255 (WHP), 2005 U.S. Dist. LEXIS 21748 (S.D. N.Y. Sept. 30, 2005)...…….....26

De Leon v. Perry, 975 F. Supp. 2d 632 (W.D. Tex. 2014) …….....26

FTC v. LabMD, No. 1:12-cv-3005-WSD, Dkt. No. 23 (N.D. Ga. Nov. 26, 2012)……..31

FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014)……..……11

Housworth v. Glisson, 485 F. Supp. 29 (N.D. Ga. 1978)……29

Khan v. Children's Nat'l Health Sys., Civ. No. TDC-15-2125, 2016 U.S. Dist. LEXIS 66404 (D. Md. May 18, 2016) ……15

LabMD, Inc. v. FTC, No. 14-cv-00810-WSD, 2014 U.S. Dist. LEXIS 65090 (N.D. Ga. May 12, 2014)…….11, 27

S. Div. First Premier Bank v. CFPB, 819 F. Supp. 2d 906 (D.S.D. 2011)……...…31

STATUTES

Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45…….*passim*

15 U.S.C. § 45(a) ……..13, 16

15 U.S.C. § 45(b) …….22, 24

15 U.S.C. § 45(c) ……...…27

15 U.S.C. § 45(d) ……...27

15 U.S.C. § 45(g) ……...8, 31

15 U.S.C. § 45(l) ……..25, 27

15 U.S.C. § 45(m) ……25, 27

15 U.S.C. § 45(n) ……..……11-14, 16, 20

15 U.S.C. § 53(b)……..2, 22, 30

Health Information Technology for Economic and Clinical Act ("HITECH"), 42 U.S.C. § 17921 *et seq.*……....3, 5, 11-12, 18, 22-23

Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d *et seq.*……...3, 5, 11-12, 18, 22-23, 28

28 U.S.C. § 1292(b) ……...……11

O.C.G.A. § 31-33-2……..……..19

REGULATIONS

16 C.F.R. § 3.43(b)(1)……19

16 C.F.R. § 3.56(c)……1, 8-9

16 C.F.R. § 4.4(a)(1)…….8

42 C.F.R. § 493.1105……..19

FEDERAL REGISTER

Health Insurance Reform: Security Standards, Final Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003)..….3

Breach Notification for Unsecured Protected Health Information, Interim Final Rule, 74 Fed. Reg. 42,740 (Aug. 24, 2009) …….....3, 22

Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) …….....3

Adjustment of Civil Monetary Penalty Amounts, Interim Final Rule, 81 Fed. Reg. 42,476 (June 30, 2016) …….....25, 27

ADMINISTRATIVE MATERIALS

Dissenting Statement of Commissioner Joshua D. Wright, *In the Matter of Apple, Inc.*, FTC File No. 1123108 (Jan. 15, 2014) ……..……21

Final Order, *In the Matter of LabMD, Inc.*, No. 9357 (July 28, 2016)……..*passim*

Initial Decision, *In the Matter of LabMD, Inc.*, No. 9357 (Nov. 13, 2015)……..*passim*

Opinion of the Commission, *In re N.C. Bd. of Dental Examiners*, No. 9343, 2011 FTC LEXIS 290 (Dec. 7, 2011)..……...……12

Opinion of the Commission, *In re Rambus, Inc.*, No. 9302, 2006 FTC LEXIS 101 (Aug. 20, 2006)……..15

Opinion of the Commission, *In re Telebrands Corp.*, No. 9313, 140 F.T.C. 278, 2005 FTC LEXIS 178 (2005)…….……...19, 21

Opinion of the Commission, *In the Matter of LabMD, Inc.*, No. 9357 (July 28, 2016)……*passim*

Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision, *In the Matter of LabMD, Inc.*, No. 9357 (May 19, 2014)……..5, 12, 18, 28

Order Denying Respondent LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.*, No. 9357 (Jan. 16, 2014)…….3, 5, 10-11, 18, 22-23, 28

Order Extending Deadlines for Filing Petition for Reconsideration and Answer Thereto, *In the Matter of LabMD, Inc.*, No. 9357 (Aug. 12, 2016)……9

Order Granting Application for Stay of Part IV of Order, *In re Novartis*, 128 F.T.C. 233, 1999 FTC LEXIS 211 (1999)……10, 25

Order Granting in Part and Denying in Part Respondent's Motion for Stay of Final Order Pending Appeal, *In the Matter of Rambus, Inc.*, No. 9302, 2007 FTC LEXIS 30 (Mar. 16, 2007)……9

Order Granting Partial Stay, *In re Toys "R" Us*, No. 9278, 126 F.T.C. 695, 1998 FTC LEXIS 224 (Dec. 1, 1998) (Appendix)……..25

Order Granting Respondent's Application to Stay Final Order Pending Judicial Review, *In the Matter of ECM Biofilms, Inc.*, No. 9358 (Dec. 8, 2015)…….…….8-9, 12

Order on Respondent's Application for Stay of Order Pending Review By U.S. Court of Appeals, *In the Matter of North Carolina Board of Dental Examiners*, No. 9343 (Feb. 10, 2012)……9, 30

Order Granting Partial Stay of the Commission's March 25, 1996, Order Against CDA, *In the Matter of California Dental Assoc., Inc.*, No. 9259, 1996 FTC LEXIS 277 (May 22, 1996)……9

Partial Dissent of Commissioner Ohlhausen, *In the Matter of ECM Biofilms, Inc.*, No. 9358 (Oct. 19, 2015) ……20

Unfairness Statement, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2 (1984).....13, 21

OTHER AUTHORITIES

AMA Ethics Op. 7.05…….19

Federal Trade Commission, Operating Manual, Ch. 11 (Judicial Enforcement)……22

Joshua Wright, Commissioner, Federal Trade Commission, Section 5 Revisited: Time for the FTC to Define the Scope of Its Unfair Methods of Competition Authority (Feb., 26, 2015)……...24, 27

WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY (1988)……13

RECORD REFERENCES AND GLOSSARY

ALJ — FTC Chief Administrative Law Judge D. Michael Chappell

CA Tr. — Closing Argument Transcript (September 16, 2015) (excerpt attached as Exhibit 1)

CC — Complaint Counsel

CCPB — Complaint Counsel's Pretrial Brief (excerpt attached as Exhibit 2)

CCAB — Complaint Counsel's Appeal Brief (excerpt attached as Exhibit 3)

CCRB— Complaint Counsel's Reply Brief to Respondent's Answering Brief (excerpt attached as Exhibit 4)

CC Statement of Facts — Complaint Counsel's Separate and Concise Statement of Material Facts as to Which There Exist Genuine Issues for Trial (May 7, 2014) (excerpt attached as Exhibit 5)

"Commission Opinion" or "Op." — Opinion of the Commission, *In the Matter of LabMD, Inc.*, No. 9357 (July 28, 2016) (attached as Exhibit 6).

Commission Order Extending Deadlines — Order Extending Deadlines for Filing Petition for Reconsideration and Answer Thereto, *In the Matter of LabMD, Inc.*, No. 9357 (Aug. 12, 2016) (attached as Exhibit 7)

"Compl." or Complaint — Complaint, *In the Matter of LabMD, Inc.*, No. 9357 (Aug. 28, 2013) (attached as Exhibit 8)

CX194 — Managed Data Solutions Project Proposal, LabMD Websense (April 11, 2011) (attached as Exhibit 9)

CX195 — Managed Data Solutions Project Proposal, LabMD Websense Time Portion (April 11, 2011) (attached as Exhibit 10)

CX448 — LabMD Access Letter Response by Dana Rosenfeld (May 31, 2011) (excerpt attached as Exhibit 11)

CX679 — Verified Complaint for Declaratory and Injunctive Relief, *LabMD, Inc. v. FTC*, No. 14-cv-00810-WSD (N.D. Ga. Mar. 20, 2014) (ECF copy attached as Exhibit 12)

Martin Dep. — Deposition Transcript of Jeff Martin (excerpt attached as Exhibit 13)

CX738 — Expert Report of Dr. Clay Shields (excerpt attached as Exhibit 14)

CX740 — Expert Report of Raquel Hill (attached as Exhibit 15)

CX741 — Expert Report of James Van Dyke (excerpt attached as Exhibit 16)

CX742 — Expert Report of Richard Kam (excerpt attached as Exhibit 17)

Daugherty Decl. — Declaration of LabMD, Inc. President and Chief Executive Officer Michael J. Daugherty in Support of Respondent LabMD, Inc.'s Application for Stay of Order Pending Review in U.S. Court of Appeals (attached as Exhibit 18)

Daugherty Decl., Ex. A — Plaintiff's Motion to Stay, *Boback v. LabMD et al.*, Civ. No. GD-14-016497 (Ct. Common Pls. Allegheny County, PA) (excerpt attached as Exhibit A to Daugherty Decl.)

Daugherty Decl., Ex. B — August 25, 2016, Motion Hearing Transcript, *Boback v. LabMD et al.*, Civ. No. GD-14-016497 (Ct. Common Pls. Allegheny County, PA) (excerpt attached as Exhibit B to Daugherty Decl.)

FPH Tr. — Final Pretrial Hearing Transcript, *In the Matter of LabMD, Inc.*, No. 9357 (May 15, 2014) (excerpt attached as Exhibit 19).

"ID" or "Initial Decision" — Initial Decision ("ID"), *In the Matter of LabMD, Inc.*, No. 9357 (Nov. 13, 2015) (attached as Exhibit 20)

HHS — U.S. Department of Health and Human Services

HIPAA — Health Insurance Portability and Accountability Act of 1996

HITECH — Health Information Technology for Economic and Clinical Health Act

IDF — Numbered Findings of Fact in the ALJ's Initial Decision

IPH Tr. — Initial Pretrial Hearing Transcript, *In the Matter of LabMD, Inc.*, No. 9357 (Sept. 25, 2013) (excerpt attached as Exhibit 21)

January 16 Order — Commission Order Denying Respondent LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.*, No. 9357 (Jan. 16, 2014) (attached as Exhibit 22).

LabMD MSD Reply — Respondent LabMD Inc.'s Reply in Support of Motion for Summary Decision, *In the Matter of LabMD, Inc.*, No. 9357 (May 12, 2014) (attached as Exhibit 23)

LabMD MTD Reply — Respondent LabMD Inc.'s Reply to Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice And to Stay Administrative Proceedings, *In the Matter of LabMD, Inc.*, No. 9357 (Dec. 2, 2013) (attached as Exhibit 24)

May 19 Order — Commission Order Denying Respondent LabMD's Motion for Summary Decision, *In the Matter of LabMD, Inc.*, No. 9357 (May 19, 2014) (attached as Exhibit 25)

Motion to Dismiss — Respondent LabMD Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, *In the Matter of LabMD, Inc.*, No. 9357 (Nov. 12, 2013) (attached as Exhibit 26)

Motion for Summary Decision — Respondent LabMD Inc.'s Motion for Summary Decision, *In the Matter of LabMD, Inc.*, No. 9357 (April 21, 2014) (attached as Exhibit 27)

PHI — Protected Health Information, as defined by HIPAA and HHS regulations.

OA Tr. — Transcript of Oral Argument, *In the Matter of LabMD, Inc.*, No. 9357 (March 8, 2016) (excerpt attached as Exhibit 28)

Order — Final Order, *In the Matter of LabMD, Inc.*, No. 9357 (July 28, 2016) (attached as Exhibit 29)

RFF — Respondent LabMD, Inc.'s Corrected Proposed Findings of Fact (August 11, 2015) (attached as Exhibit 30)

RX412 — LabMD Data-Security Expenditures Chart (attached as Exhibit 31)

RX526 — Complaint Counsel's Amended Response to LabMD, Inc.'s First Set of Requests for Admission (Numbers 1-20) (Apr. 4, 2014) (attached as Exhibit 32)

RX532 — Deposition Transcript of Testimony of Daniel Kaufman (May 12, 2014) (attached as Exhibit 33)

RX533 — Expert Report of Adam Fisk (attached as Exhibit 34)

RX644 — STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113TH CONG., TIVERSA, INC.: WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015) (prepared for Chairman Darrell E. Issa) (attached as Exhibit 35)

RX649 — "Meanwhile, Back In Court (Updated)," PHIPRIVACY.NET (SEPT. 9, 2013) (attached as Exhibit 36).

Tr. — Transcript of evidentiary hearing before the ALJ (excerpts attached as Exhibit 37)

I. INTRODUCTION

A stay "application shall address the likelihood of the applicant's success on appeal, whether the applicant will suffer irreparable harm if a stay is not granted, the degree of injury to other parties if a stay is granted, and why the stay is in the public interest." 16 C.F.R. § 3.56(c).

A stay is warranted in this case because all four stay factors are met.

The first stay factor is satisfied for two reasons. *First*, the factual record is voluminous, complex, and spans a period of at least ten years. This matter also involves several novel bases for decision, all of which invite alternative conclusions—as demonstrated by the divergent conclusions reached by Chief Administrative Law Judge D. Michael Chappell ("Chief ALJ Chappell" or "ALJ"), who dismissed the administrative complaint in its entirety, and the Commission, which reversed the Initial Decision and imposed liability on a different legal theory. The Commission itself has recognized the fundamental issues presented, as have federal courts. *Second*, although the Commission need not address the likelihood that LabMD's petition for review will be granted to stay its Order, LabMD is likely to succeed on the merits because, *inter alia*, the Commission Opinion and Order are *ultra vires*, violate due process, are unsupported by substantial evidence, and are otherwise contrary to law.

The second stay factor is also satisfied for two reasons. *First*, the Order requires LabMD to hire third-party contractors, conduct research, and perform a variety of other burdensome, expensive, time-consuming tasks that would involve substantial compliance costs—costs that LabMD has no ability to pay and that, even if LabMD could afford them, would be unrecoverable due to FTC's sovereign immunity. That is irreparable harm as a matter of law. *Second*, the Commission Opinion and Final Order irreparably harm LabMD by violating its constitutional rights, harming its reputation, and irreparably and irredeemably causing direct and indirect harm, prejudice, and damage to LabMD's appeal rights.

The third and fourth stay factors—risk of harm to the consumers and the public interest—also favor LabMD.

A stay will not harm anyone. There is no evidence that the alleged unfair practices at issue here caused economic or any other concrete physical or monetary harm to any identifiable person. The Commission does not dispute this. Complaint Counsel has not identified a single consumer victim after *eight* years,[1] instead relying solely on speculative, methodologically flawed expert testimony divorced from the facts of this case to show harm. There is no danger that LabMD's alleged computer data-security practices between 2005 and 2010 will harm anyone or reoccur, as LabMD is no longer operational and its computers are not even turned on, let alone connected to the Internet.

If the Commission believed LabMD's data-security practices posed a time-sensitive public threat, it should have sought temporary injunctive relief in federal district court pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), no later than August 2013, when the Complaint was issued. (FTC staff began investigating LabMD in January 2010.) The Commission did not do this, instead *electing* to proceed through its administrative process, which does not authorize temporary relief. The Commission decision to prosecute LabMD in-house three-and-a-half years after initiating its investigation underscores why a stay will harm no one.

Finally, it is always in the public interest to ensure that the Commission Opinion and Final Order comply with the United States Constitution and other federal law.

---

[1] Due to the ever-changing "relevant time period" adopted by FTC, the failure to identify any victims in this case may well be eleven (11) years now. LabMD, however, objects to this elastic time period, as repeatedly asserted before the Commission and the ALJ. *See, e.g.*, FPH Tr. 44:7-46:14; OA Tr. 58-59.

All stay factors favor LabMD. Accordingly, as further explained below, the Commission should grant LabMD's stay application.

II. BACKGROUND

LabMD was a cancer-detection business subject to detailed medical data-security standards set by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Department of Health and Human Services ("HHS") regulations.[2] *See* Op. 12 & n.22; RFF 7-11, ¶¶ 12-34. The FTC does not enforce HIPAA, HITECH, and HHS regulations establishing medical data-security standards. January 16 Order at 12.

The irregular circumstances surrounding the FTC investigation of LabMD and its principal "evidence" of harm are discussed at length in the Initial Decision, in which Chief ALJ Chappell made findings of fact and credibility determinations based on first-hand observations of witness demeanor. *See* IDF 100-181; *see also* RFF 4-7, 11-31, ¶¶ 1-10, 35-85; RX644.

The genesis of this case is a crime and a lie—its psychogenesis is misrepresentation, fraud, and entitled arrogance. In 2008, Tiversa stole a LabMD file (the "1718 File") containing Protected Health Information ("PHI") subject to HIPAA from a LabMD workstation in Atlanta, Georgia, as part of a scheme to extort business. Tiversa repeatedly contacted LabMD to sell LabMD its "remediation" services. LabMD refused to pay. *See* IDF 100-130.

In 2009, in retaliation against LabMD for refusing its "services," Tiversa transferred the 1718 File to FTC Complaint Counsel Alain Sheer and other FTC Staff through a shell company,

---

[2] *See, e.g.*, 65 Fed. Reg. 82,462 (Dec. 28, 2000)(HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334 (Feb. 20, 2003)(HHS's HIPAA Security Rule). After September 2009, LabMD was subject to the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the HHS Breach Notification Rule. *See* 74 Fed. Reg. 42,740 (Aug. 24, 2009)(HHS Interim HITECH Rule).

the Privacy Institute, which was jointly created by FTC and Tiversa for that purpose. *See* IDF 131-45.

In fall 2009, Tiversa representatives, including then-Tiversa CEO Robert Boback and Richard Wallace, met with Mr. Sheer and other FTC Staff in Washington, D.C., to discuss the file transfer. IDF 145. After the meeting, "based on statements of Mr. Boback, Mr. Wallace understood that Tiversa needed to increase the apparent 'spread' of the files identified on the list provided to the FTC pursuant to the CID." IDF 146; *accord* Op. 32 n.84 ("The ALJ found … that after the meeting between Tiversa and FTC staff …, Mr. Boback directed Mr. Wallace to generate false information purporting to show that the 1718 File had spread to multiple locations on the Internet…."). Thereafter, Mr. Wallace fabricated evidence that the LabMD 1718 File hacked from Atlanta, Georgia, had "spread" across the Internet to places such as Apache Junction, Arizona, even though it was not true.[3] IDF 149.

In January 2010, "the FTC commenced its investigation into LabMD's data security practices …, based upon Tiversa's claim that the 1718 File, containing personal information, had been disclosed by means of a peer to-peer file-sharing network." ID 6; *see also* Tr. 31.

On August 28, 2013, the Commission issued a one-count administrative complaint against LabMD solely alleging that LabMD's medical data-security practices constituted "unfair" trade

[3] The FBI raided Tiversa headquarters in Pittsburgh, Pennsylvania, on March 1, 2016. Daugherty Decl., Ex. A at 6 ("Pending FBI Criminal Investigation"). At a hearing in a Pennsylvania state court on August 25, 2016, in a defamation case filed by Tiversa and Boback against LabMD and Mr. Daugherty several years ago, Tiversa's former CEO, Robert Boback, asked that Court to stay his case because, due to the impending FBI investigation of Boback, Boback might have to plead his right against compelled self-incrimination under the Fifth Amendment. Boback's criminal defense attorney, Robert Ridge, disclosed to the Court during that hearing that he met with a DoJ prosecutor in Washington, D.C., on August 10, 2016, to discuss the investigation of Boback. The DoJ prosecutor told Ridge that the FBI was investigating Boback because of his communications (i.e., misrepresentations) to the federal government, including Boback's statements to the FTC and Congress. Daugherty Decl., Ex. B at 7:9-12:2, 21:16-24.

practices banned by Section 5 of the FTC Act.[4] The Complaint included allegations relating to the 1718 File and Tiversa. *See* Compl. ¶ 17. But it did not allege that LabMD's medical data-security practices violated data-security standards set by HIPAA and HITECH, which are exclusively enforced by HHS and state attorneys general. HHS did not join the FTC prosecution of LabMD. RX649. Complaint Counsel and the Commission subsequently confirmed that LabMD was not accused of violating HIPAA or HITECH. *See* January 16 Order at 12 ("[T]he Commission cannot enforce HIPAA and does not seek to do so."); May 19 Order at 5 (the FTC has not accused LabMD of violating HIPAA, HITECH, and/or HHS medical data-security regulations; "this case has nothing to do with HIPAA").

In January 2014, LabMD was forced to wind down its operations because of FTC's prosecution and destruction of the company. *See* IDF 38; RFF 115-20, ¶¶ 507-20. At that time, LabMD stopped accepting specimen samples and conducting tests. IDF 38. LabMD's financial condition is now beyond repair. *See* Daugherty Decl. ¶¶ 3-8, 19, 23. It has de minimis assets and no revenue. *Id*. ¶¶ 5-8. Its 2015 tax return, for example, showed substantial losses and a substantially negative net worth. *Id*. ¶ 6. It has no prospect of resuming its business and it has no ability to pay the substantial costs entailed in complying with the Order. *Id*. ¶¶ 3-8, 19, 22-23.

In May 2014, an evidentiary hearing was held before Chief ALJ Chappell. ID 5. In its opening statement, Complaint Counsel stated that it did not plan to introduce evidence that LabMD's alleged data-security practices harmed any consumers.[5] Tr. 13:23-14:3 ("JUDGE CHAPPELL: … [Y]ou don't plan to introduce evidence of harm, but your position is that doesn't

---

[4] The "Complaint does not allege that Respondent committed a 'deceptive act or practice' in violation of Section 5(a) of the FTC Act…." RX0526 at 6 (Resp. to RFA ¶ 4).

[5] *See also* CA Tr. 12:10-11 ("[Complaint Counsel]: We did not present a consumer witness in this case, Your Honor.").

mean no harm occurred? Is that what you said? MR. SHEER: That's correct."). Complaint Counsel did not present any evidence of actual harm to any consumer, ID 52, instead relying on materials and testimony provided by Tiversa to support its claim that the LabMD file had "spread" across the Internet, thereby harming consumers. *See, e.g.,* CCPB, Ex. 2 at 10; Tr. 16-17, 31 (CC opening statement); CX0740 (Hill Expert Report) at 20 ¶ 49 (citing Boback for proposition that the 1718 File was found in four places); CX0742 (Kam Expert Report) at 6, 9, 18-19 (same); Tr. 408-416 (same); CX0741 (Van Dyke Expert Report) at 2, 7-8 (same); Tr. 667-669, 736 (same); Tr. 904-06 (Shields) (considered Boback deposition).[6]

After Complaint Counsel rested its case-in-chief, Richard Wallace, a witness for Respondent, invoked his Fifth Amendment privilege against compelled self-incrimination. ID 8-9. The ALJ stayed the case to allow Mr. Wallace to obtain immunity from criminal prosecution. ID 9. On May 5, 2015, Mr. Wallace's testimony revealed that FTC's case was predicated on perjured testimony and fabricated evidence that the 1718 File had "spread" on the Internet via LimeWire.[7] *See* IDF 100-168; Op. 31 ("Mr. Boback's assertion that Tiversa gathered evidence showing that the 1718 File had spread to multiple Internet locations by means of LimeWire was false…."); Tr. 1380-1388, 1441-1444.

---

[6] Tiversa's false evidence fatally infected this entire case. Even LabMD expert Adam Fisk relied on it: the conclusions of his report are based on the (false) *assumption* the 1718 File was found at four IP addresses outside of Atlanta, Georgia. *See* RX533 at 24. Tiversa thus infected Fisk's report, which, in turn, poisoned that of Complaint Counsel's *rebuttal* expert (to Mr. Fisk), Clay Shields, whose report and testimony—among many other shortcomings, *see* RFF 107-108, ¶¶ 469-478—*rebutted conclusions predicated on false information*. *See* CX738 at 1, 11-31. In turn, the Commission Opinion mistakenly relies on Shields, whose *rebuttal* report and testimony are predicated on this false evidence and testimony. *See, e.g.,* Op. 21-23.

[7] The Initial Decision noted this "led to the unusual result of Complaint Counsel retreating from its own evidence—evidence upon which it had relied in substantial part to support its claim of consumer injury in this case…." ID 6. *Cf.* Tr. 1227-1229.

In November 2015, the ALJ issued an Initial Decision dismissing the Complaint in its entirety for lack of evidence of actual or likely harm to consumers. ID 88. The ALJ concluded that "[t]he record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged failure to employ 'reasonable' data security for its computer networks[.]"[8] ID 52. Instead, Complaint Counsel's theory of harm "is predicated on expert opinion that essentially only theorizes how consumer harm could occur." ID 53.

The Initial Decision found that Complaint Counsel's expert reports and testimony relied on false testimony and fabricated evidence and/or were based on speculation and thus entitled to little or no weight. *See* ID 7-11 (Complaint Counsel's experts relied on false evidence and testimony), 61, 68, 76, 79 (Kam conclusions entitled to little or no weight), 64, 66 (Van Dyke testimony described as "speculation"), 64, 80 (Van Dyke testimony described as "unpersuasive"). *Accord* RFF 73-108, ¶¶ 313-478. The Initial Decision further stated:

> [T]he absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years, undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless "likely" to occur.… Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.

ID 52-53. The ALJ also found that "whatever risk might be inherent in Respondent's alleged 'unreasonable' data security during the Relevant Time Period, the record is devoid of expert opinion as to the degree of risk beyond that period," *i.e.*, since July 2010—over six years ago. ID 87 n.45.

---

[8] FTC staff began its investigation of LabMD no later than January 2010 and took extensive discovery from LabMD and numerous third parties during its investigation and this adjudication. *See generally* ID 5-11 & n.4.

On July 28, 2016, the Commission found in favor of itself by reversing the Initial Decision and issuing an Opinion and Final Order against LabMD. *See* Op.; Order. The Commission Opinion acknowledged the absence of any evidence of harm to any identifiable person allegedly caused by LabMD's allegedly "unreasonable" medical data-security practices. *See* Op. 17. Nonetheless, it found that LabMD's alleged medical data-security practices were "unreasonable." Op. 1. *But see* RFF 31-68, ¶¶ 86-288 (LabMD data-security practices); RX0533 (Fisk Expert Report). The Commission further held that abstract amorphous privacy harms caused by Tiversa's theft of the 1718 File and the alleged "exposure" of the 1718 File on LimeWire[9] sufficed to show that LabMD's medical data-security practices "causes or is likely to cause substantial injury to consumers." *See* Op. 16-25.

"Commission[] cease and desist orders … take effect 'upon the sixtieth day after such order is served,' unless 'stayed … by … the Commission' or 'an appropriate court of appeals of the United States.'" Order Granting Respondent's Application to Stay, *In the Matter of ECM Biofilms, Inc.*, No. 9358, at 1-2 (Dec. 8, 2015) (quoting 15 U.S.C. § 45(g)(2)).

Service of the Commission's Opinion and Final Order pursuant to Rule 4.4(a)(1)(ii-iii), 16 C.F.R. § 4.4(a)(1)(ii-iii), was accomplished on August 1, 2016. Absent a stay, the Order will become effective on September 30, 2016.

III. STANDARD FOR STAY PENDING REVIEW

"Under Commission Rule 3.56(c) an application for stay must address the following four factors: (1) the likelihood of the applicant's success on appeal; (2) whether the applicant will suffer

[9] No evidence of "exposure" or "disclosure" exists. In fact, Richard Wallace never testified that he accessed the 1718 File through LimeWire. Moreover, the 1718 File being "available for sharing" and being in a state of exposure by a download or being "pulled down" are explicitly distinct actions. *See* IDF 66 (citing Shields, Tr. 891-892). That leaves only the false "spread" of the 1718 File, which was and remains the death knell for the government's case against LabMD.

irreparable harm absent a stay; (3) the degree of injury to other parties if a stay is granted; and (4) whether the stay is in the public interest." *In the Matter of ECM Biofilms, Inc.,* No. 9358, at 1-2 (citing 16 C.F.R. § 3.56(c)).

A. LIKELIHOOD OF SUCCESS ON APPEAL

The first stay factor is satisfied on two independent bases: due to the extensive and complex record in this matter and the important issues presented, and because LabMD is likely to prevail on the merits of its appeal.

1. This Case is Based on A Complex Factual Record and Raises Important Issues

"[T]he first stay factor can be substantially satisfied by a showing that the Commission's decision was based on a complex factual record." *In the Matter of Rambus, Inc.,* No. 9302, 2007 FTC LEXIS 30, at *8 (Mar. 16, 2007); *see, e.g., In the Matter of ECM Biofilms, Inc.,* No. 9358, at 1-2 (granting stay because "issues … are sufficiently complex"). A stay is also appropriate where, as here, a case presents important unresolved legal questions, even if there is some potential harm to consumers *and even if the Commission believes its decision is correct*. *See In the Matter of North Carolina Board of Dental Examiners,* No. 9343, at 4 (Feb. 10, 2012) (granting stay because "case presents an important unresolved legal question"). The Commission may grant a stay without questioning the merits of its Opinion. *In the Matter of California Dental Assoc., Inc.,* No. 9259, 1996 FTC LEXIS 277, *10 (May 22, 1996).

Both tests are independently met here. The Commission has acknowledged ***"the extensive and complex record in this matter and the important issues presented."*** Commission Order Extending Deadlines (emphasis added). Accordingly, the first stay factor is satisfied as a matter of law.

Additionally, the factual record is sufficiently complex to support a stay. *See* RFF 4-120, ¶¶ 1-523. The case spans many years: FTC staff commenced its investigation in January 2010, based on events in 2008; the Commission issued its Opinion and Order on July 28, 2016. It is also voluminous. *See* ID 6 ("Proceedings in this matter have been lengthy, with over 200 entries on the docket[.]"). During the evidentiary hearing, "[o]ver 1,080 exhibits were admitted into evidence, 39 witnesses testified, either live or by deposition, and there are 1,504 pages of trial transcript. The parties' proposed findings of fact and conclusions of law, post-trial briefs, replies to proposed findings of fact and conclusions of law, and reply briefs total 2,066 pages." ID 5 n.4.

"[A]rguable difficulties arising from the application of the law to a complex factual record can support a finding that a stay applicant has made a substantial showing on the merits." *In re Novartis*, 128 F.T.C. 233, 1999 FTC LEXIS 211, *5 (1999). Here, the divergence between the Initial Decision dismissing the Complaint and the Commission Opinion imposing liability showcases those difficulties and why this test is met here. For instance, the Initial Decision and Commission Opinion sharply disagreed as to how Section 5(n)'s substantial injury element should be interpreted. *Compare, e.g.,* ID 14, 54-55, 69, 85, 90 & n.43, *with* Op. 17-21 (rejecting ALJ legal analysis). Likewise, the Initial Decision and Commission Opinion reached contrary conclusions on factual and evidentiary issues, such as the appropriate weight given to Complaint Counsel's harm experts. *Compare, e.g.,* ID 55-65, *with* Op. 21-25 (rejecting ALJ evaluation of Complaint Counsel's evidence and harm experts).

This case also presents important unresolved legal questions. The Commission unanimously stated that "[t]his case presents fundamental questions about the authority of the

Federal Trade Commission … in the increasingly important field of data security."[10] January 16 Order at 1. Courts have previously recognized that whether the FTC has Section 5 "unfairness" data-security authority, and, if so, whether the agency provided adequate notice of what data-security practices it thinks Section 5 requires or prohibits, are questions that "give rise to a substantial difference of opinion."[11] *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 634 (D.N.J. June 23, 2014). "[G]iven the novelty of liability issues relating to data-security breaches, … reasonable jurists may differ over the … resolution of" these "novel, complex statutory interpretation issues."[12] *Id.*

In addition, this case presents at least five additional complex questions of first impression. *First*, whether the FTC may exercise Section 5 "unfairness" jurisdiction over HIPAA-covered healthcare providers' data security. *Second*, whether the FTC provided adequate notice of what medical-industry data-security standards it thinks HIPAA-covered entities like LabMD must comply with during the Relevant Time Period of January 2005-July 2008[13] that are different from and more rigorous than those set by HIPAA. *Third*, whether the alleged "disclosure of sensitive medical information alone, in the absence of proven economic or physical harm" can be actual harm that "satisfies the 'substantial injury' requirement" of Section 5(n). *See* Op. 17. *Fourth*,

---

[10] *Accord LabMD, Inc. v. FTC*, No. 14-cv-00810-WSD, 2014 U.S. Dist. LEXIS 65090, *16 n.6 (N.D. Ga. May 12, 2014) ("[T]he authority of the FTC to enlarge its regulatory activity in the data security area presents an interesting and likely important jurisdictional issue….").

[11] The Third Circuit granted interlocutory review of these issues under 28 U.S.C. § 1292(b). *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015).

[12] Only the Third Circuit has addressed these general issues under factually and legally distinguishable circumstances; other Circuits may reach contrary conclusions.

[13] "The evidence shows that the 1718 File was available for peer-to-peer sharing through LabMD no earlier than June 2007 (the date of the document) until May 2008, when Respondent removed LimeWire from the Billing Computer. … [T]he evidence fails to show that the 1718 File was in fact downloaded by anyone other than Tiversa, who obtained the document in February 2008." ID 60 (citations omitted).

whether an alleged "privacy harm," standing alone, can be actual harm sufficient to constitute "substantial injury" under Section 5(n). *See* Op. 19. *Fifth*, the meaning of "likely to cause substantial injury" under Section 5(n). *See* Op. 20.

Thus, "the issues in this case are sufficiently complex to tend to support a stay pending appeal." Order Granting Respondent's Application to Stay Final Order, *In the Matter of ECM Biofilms, Inc.*, FTC No. 9358, at 2.

2. LabMD Is Likely To Succeed On Petition for Review

The first stay factor is independently met here because it is likely that LabMD's petition for review will be granted for at least nine reasons.[14]

i. Commission Erroneously Denied LabMD's Dispositive Motions and Wrongly Rejected LabMD's Jurisdictional and Facial and As-Applied Due Process Arguments

LabMD continues to object to the Commission Order Denying LabMD's Motion to Dismiss ("January 16 Order") and Order Denying Respondent LabMD's Motion for Summary Decision ("May 19 Order"). For the reasons set forth in Respondent's Motions and in related briefing, attached as Exhibits 23-24 & 26-27, the Commission reversibly erred when it, *inter alia*, rejected LabMD's jurisdictional and due process arguments.[15] *See* May 19 Order at 9-10; *see also* ID 46.

The FTC does not have Section 5 "unfairness" jurisdiction over medical data-security practices subject to standards set by HIPAA, HITECH, and HHS regulations. First, the FTC does not have Section 5 "unfairness" jurisdiction to regulate data security and require businesses to

---

[14] This Application sets forth an illustrative, not exhaustive, list of Commission Opinion errors. It is not comprehensive, and LabMD may raise additional errors on appeal.

[15] All such issues, which could not be raised in LabMD's answering brief in response to Complaint Counsel's appeal, are now ripe for review. *See In re N.C. Bd. of Dental Examiners*, No. 9343, 2011 FTC LEXIS 290, at *23-24 (Dec. 7, 2011); *see also* May 19 Order at 9-10.

adopt what it believes to be "reasonable and appropriate" data-security practices.[16] *See* 15 U.S.C. § 45(a),(n); *La. Pub. Serv. Com. v. FCC*, 476 U.S. 355, 374-75 (1986); *Util. Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125, 133, 161 (2000). Second, the FTC lacks "unfairness" jurisdiction to regulate medical data-security practices, which are subject to security standards set by HIPAA and HITECH and enforced by HHS.[17] *See Credit Suisse Sec. (USA) LLC v. Billing*, 551 U.S. 265 (2007).

Further, the FTC failure to provide fair notice of what data-security practices it believes Section 5 prohibits or requires (particularly before July 2010) before bringing this action violates LabMD's due process rights. The FTC, "as enforcer of the Act, retains the responsibility to state with ascertainable certainty what is meant by" its putative Section 5 "unfairness" PHI data-security standards.[18] *Georgia Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005 (11th Cir. 1994). *Cf. S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273, 1283-85 (5th Cir. 1981). The Commission has not done so.[19] This lack of standards also violates due process by "authoriz[ing] and encourage[ing]

---

[16] 15 U.S.C. § 45(a)'s plain language independently limits the Commission's "unfairness" jurisdiction to business practices that are "marked by injustice, partiality, or deception," i.e., one that is "not equitable." *Webster's Ninth New Collegiate Dictionary* (1988); *see also LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010).

[17] "Of course, if matters involving health and safety are within the primary jurisdiction of some other agency, Commission action might not be appropriate." Unfairness Statement, 104 F.T.C. 949, 1984 FTC LEXIS 2, *308 n.15.

[18] The ascertainable certainty standard applies to administrative adjudications. *See Georgia Pac. Corp.*, 25 F.3d at 1005; *Trinity Broad. v. FCC*, 211 F.3d 618, 619, 628 (D.C. Cir. 2000) (license renewal).

[19] The Commission Opinion reliance on a 2007 "Guide for Business," administrative complaints, and consent orders as a source of notice fails. *See* Op. 30 n.81. As the Third Circuit explained in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015): "the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices fail § 45(n)," *id.* at 256 n.21; "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a)," *id.* at 257 n.22; and "it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees," *id.* at 257 n.23.

seriously discriminatory enforcement," *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012), as demonstrated by this case. Therefore, this action violates due process. *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926); *Giaccio v. Pa.*, 382 U.S. 399, 402-03 (1966). Further, the Commission attempt here to set data-security standards for all private businesses, including healthcare providers subject to HIPAA and HITECH, through an adjudication instead of a rulemaking is an abuse of discretion. *See Ford Motor Co. v. FTC*, 673 F.2d 1008, 1009-10 (9th Cir. 1981).

ii. **The Commission Opinion Misconstrued Section 5's Plain Language**

The Commission Opinion is contrary to the plain language of Section 5(n), 15 U.S.C. § 45(n), which, *inter alia*, requires proof that an "act or practice causes or is likely to cause substantial injury to consumers" before "unfairness" liability may be imposed.

The Commission Opinion erroneously held that purported abstract privacy harms purportedly stemming from the alleged "disclosure" of medical information—unaccompanied by any tangible injury, such as monetary harm, to anyone—constitute "substantial injury" under Section 5(n). Op. 17. *But see* ID 91 (COL ¶ 25) ("Subjective feelings of harm … do not constitute 'substantial injury[.]'"). In support, the Commission relied primarily on other statutes, court cases interpreting other statutes, FTC administrative complaints and consent orders, and the Restatement of Torts. *See* Op. 17-19. Such extensive reliance on extrinsic sources of "public policy" violates Section 5(n), which states that "public policy considerations may not serve as a primary basis for [an "unfairness"] … determination."[20] 15 U.S.C. § 45(n). Regardless, to the extent such "public policy" evidence is relevant, it confirms that evidence of actual harm to identifiable individuals in

[20] "According to the legislative history of Section 5(n), '[e]motional impact and more subjective types of harm alone are not intended to make an injury unfair.'" ID 69 (citation omitted).

the form of identity theft and fraudulent transactions is required to show injury. *See, e.g.*, *Khan v. Children's Nat'l Health Sys.*, Civ. No. TDC-15-2125, 2016 U.S. Dist. LEXIS 66404, *7-22 (D. Md. May 18, 2016) ("increased risk" of identity theft and abstract "loss of privacy" not injury-in-fact); *see Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)*; Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013).

The Commission Opinion also erred by holding that "showing a 'significant risk' of injury satisfies the 'likely to cause' standard." Op. 21. "Likely" is an undefined term and thus its ordinary meaning, as informed by dictionary definitions, controls. *See Schindler Elevator Corp. v. United States ex rel. Kirk*, 563 U.S. 401, 407-08 (2011) (courts "look first to the word's ordinary meaning," as expressed in dictionaries); ID 54-55. The ordinary meaning of "likely" is "probable" or "highly probable." *See* ID 54. The statute's plain language controls over legislative history.[21] *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992); *see also Christensen v. Harris Cnty.*, 529 U.S. 576, 587 (2000) (policy statements lack force of law); *Chamber of Commerce v. Whiting*, 131 S. Ct. 1968, 1980 (2011) (legislative history not law). Section 5(n) requires proof of actual or, at minimum, probable or highly probable economic or physical harm. *See* ID 52-53.

iii. The Commission Opinion is Unsupported By Evidence and Contrary to Law

The Commission Opinion is unsupported by substantial evidence. *See Schering-Plough Corp. v. FTC*, 402 F.3d 1056, 1062-63, 1069-71 (11th Cir. 2005). At minimum, Complaint Counsel has the burden of proving a Section 5 violation by preponderant evidence. *In re Rambus, Inc.*, No. 9302, 2006 FTC LEXIS 101, at *45 (Aug. 20, 2006). It did not do so. The Initial Decision held that "[b]ased on the totality of the evidence presented, Complaint Counsel has failed

[21] Even if relevant, the legislative history of Section 5(n) further confirms that Congress rejected the "significant risk" standard. *See* ID 54-55, 69.

to meet its burden of proving, by a preponderance of the evidence, that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury."[22] ID 92 (COL ¶ 36). The Commission determined that "the ALJ applied the wrong legal standard for unfairness" and reversed the Initial Decision, Op. 1, stating that "[u]nlike the ALJ, we agree with Complaint Counsel that showing a 'significant risk' of injury satisfies the 'likely to cause' standard," Op. 21. But the Commission did not address Complaint Counsel's burden of proof and whether it was met. Instead, the Commission uprooted *sub silentio* the ALJ's conclusion that "even under Complaint Counsel's asserted 'significant risk' standard for proving likely harm, Complaint Counsel has failed to prove that Respondent's alleged unreasonable data security is 'likely' to cause substantial consumer injury." ID 55.

In so doing, the Commission relied on *ex parte*, uncross-examined statements in a "deposition" by a former LabMD employee when LabMD's Counsel was not present "for factual descriptions of LabMD's network, equipment, and applications, as well as the day-to-day practices of LabMD's IT employees." Op. 12-13 n.28. *Cf.* RFF 31-68, ¶¶ 86-288. The Commission did this even though the Initial Decision did not cite or rely on these statements, which deserve little, if any, weight. *See* FPH Tr. 9:17-10:8. That is reversible error. *See, e.g., Schering-Plough*, 402 F.3d at 1069-71; *Rambus Inc. v. FTC*, 522 F.3d 456, 459, 469 (D.C. Cir. 2008).

Further, notwithstanding its apparent incorporation of and reliance on negligence principles as a source of "reasonableness" standards, *see, e.g.*, Op. 21, the Commission Opinion is unsupported by any expert evidence or testimony regarding the baseline standard of care for "reasonable" data security that a business of LabMD's size and nature must meet for any specific period of time. Failure to establish the applicable standard of care is fatal. *See, e.g., Silverpop Sys.*

[22] A necessary but not sufficient condition for "unfairness" liability. *See* 15 U.S.C. § 45(a),(n).

v. Leading Mkt. Techs., Inc., No. 14-14258, 2016 U.S. App. LEXIS 196, *8-9 (11th Cir. Jan. 5, 2016) (unpublished). Because Complaint Counsel did not meet its burden of establishing the applicable standard of care (and deviations therefrom at specific points in time), the Final Order cannot stand.

The Commission Opinion apparently acknowledges now that "covered entities like LabMD" look to HIPAA for data-security standards. *See* Op. 12 & n.22 ("LabMD … subject to HIPAA"). But Complaint Counsel did not introduce any expert testimony establishing what HIPAA data-security standards applied to LabMD at any point in time, what those standards required, and how and when LabMD allegedly deviated therefrom. *Cf.* January 16 Order at 14 (data-security standards "rapidly changing"). The Commission apparently (and, if so, correctly) rejected at least in part the "defense-in-depth" standards devised and proposed in early 2014 by Complaint Counsel's only expert witness on data-security standards, Dr. Raquel Hill, who stated that "[r]easonable care [for LabMD's computer networks] would be defense in depth." Tr. 310:2-6; *see* RX0532 at 203:15-19. But Dr. Hill admitted at trial that she knew little, if anything, about the *medical industry* data-security standards that the Commission apparently now acknowledges applied to LabMD: those set by HIPAA, HITECH, and HHS regulations, such as the HIPAA Privacy and Security Rules. *See* Tr. 231; *see also* Tr. 234, 306.

Thus, the record is devoid of evidence of the objective medical-industry practice standard for data-security practices customary for medical businesses of LabMD's size and nature to adopt at the time that such LabMD practices were used. *See* RFF 73-89, ¶¶ 331-385.

Nonetheless, the Commission has now reversed course without explanation, citing HIPAA as "a useful benchmark for reasonable behavior" for data security.[23] Op. 12. The Commission's newfound reliance on HIPAA standards without notice to LabMD, as an evolving theory of liability, contradicts its earlier statements, as well as those of Complaint Counsel,[24] on the role HIPAA data-security standards played in this case. *Cf. Rodale Press, Inc. v. FTC*, 407 F.2d 1252, 1256-57 (D.C. Cir. 1968) (agency cannot change theory of liability midstream without notice). It is also unsupported by evidence.

If the Commission intended to hold LabMD to HIPAA data-security standards, the need for expert testimony on HIPAA is indispensable given that "the Commission cannot enforce HIPAA and does not seek to do so," January 16 Order at 12, and lacks HIPAA and medical-industry expertise.[25] *Cf. Department of Treasury v. FLRA*, 837 F.2d 1163, 1167 (D.C. Cir. 1988) (no deference owed "when…agency interprets…statute other than that which it has been entrusted to administer"). This also violates due process, as applied to LabMD, because the Commission did not carry *its burden* of establishing the constitutionally required standard of care under HIPAA and industry practice through expert testimony. *See S&H Riggers*, 659 F.2d at 1283-85; *Fla. Mach. & Foundry, Inc. v. OSHRC*, 693 F.2d 119 (11th Cir. 1982) (industry-specific standards control); *B&B Insulation v. OSHRC*, 583 F.2d 1364, 1370 (5th Cir. 1978) (same).

---

[23] *See also* OA Tr. 46:19-23 ("COMMISSIONER McSWEENY: Aren't we talking about HIPAA-covered documents, medical records, and hopefully state standards here as well? [LabMD Counsel]: Well, that's just the point. Professor Hill said she was not familiar with HIPAA.").

[24] *See, e.g.*, January 16 Order at 12 & nn.19-20; May 19 Order 4-6; CCRB 5; CC Statement of Facts at 10-11.

[25] For example, Complaint Counsel actively frustrated LabMD's effort to over-comply with HIPAA/HITECH notification obligations during the Part 2 investigation. Tr. 1020-1021, 1027.

Indeed, the Commission faulted LabMD for not destroying or deleting medical records, *see* Op. 1, 4, even though LabMD is required to preserve these records and samples by law. *See* O.C.G.A. § 31-33-2(a)(1)(A) (ten-year record-retention requirement for healthcare providers); 42 C.F.R. § 493.1105 (CLIA record-retention requirements). By implication, Section 5 compliance requires LabMD to violate Georgia patient-protection law, thereby causing a significant risk of concrete harm to referring physicians' patients by depriving them of access to their medical data.[26] *Compare* Tr. 1031, *with* AMA Ethics Op. 7.05 (ethical obligation to retain medical records).

iv. **The Commission Opinion Erroneously Ignored Initial Decision's Evaluation of Complaint Counsel's Harm Experts.**

The Commission erred when it ignored the ALJ's factual findings and the weight he assigned to Complaint Counsel's expert opinions after personally observing the demeanor of these witnesses at the evidentiary hearing. *See, e.g.*, *Schering-Plough*, 402 F.3d at 1069-71. The Commission wrongly rejected (without adequate explanation) the Initial Decision's determination that expert testimony on consumer harm was speculative, methodologically flawed, and/or based on fabricated testimony and false evidence and thus entitled to little or no weight.

Expert evidence should only be given weight if the methodology is sound and based on more than speculation divorced from the facts of a case. *See In re Telebrands Corp.*, 140 F.T.C. 278, 312 n.37 (Sept. 19, 2005) ("spirit of Daubert" applies); 16 C.F.R. § 3.43(b)(1) (unreliable and immaterial evidence should be excluded); *see also Pasha v. Gonzales*, 433 F.3d 530, 535 (7th Cir. 2005) ("'[j]unk science' has no … place in administrative proceedings"). Here, the ALJ accorded little or no weight to speculative expert testimony on harm. *See* ID 7-11 (Complaint Counsel's

[26] This further confirms the irreconcilable conflict between medical-industry-specific standards and FTC Section 5 "unfairness unreasonableness."

experts relied on false evidence and testimony), 61, 68, 76, 79 (Kam conclusions entitled to little or no weight), 64, 66 (Van Dyke testimony described as "speculation"), 64, 80 (Van Dyke testimony described as "unpersuasive"). *See generally Libas, Ltd. v. United States*, 193 F.3d 1361, 1366 (Fed. Cir. 1999). The Commission erroneously ignored the Initial Decision's assessment of Complaint Counsel's harm experts. *Cf.* Partial Dissent of Commissioner Ohlhausen, *In the Matter of ECM Biofilms, Inc.*, No. 9358, at 3-4 (Oct. 19, 2015).

v. FTC Staff's Relationship with Tiversa Violates Fourth Amendment

The Commission Opinion glossed over the troubling relationship between FTC staff and a third party, Tiversa, which provided false evidence and testimony to support Complaint Counsel's claim that the 1718 File "spread" to other locations on the Internet. *See* Op. 31-32 & nn.83-84; IDF100-168; RFF 1-7, 11-31, ¶¶ 1-11, 35-85; RX644. The 1718 File is the linchpin of the Commission Opinion argument that LabMD data security harmed or was likely to harm consumers. *See* Op. 17-26. The Commission's reliance on the stolen 1718 File violates LabMD's Fourth Amendment rights. *See Knoll Associates, Inc. v. FTC*, 397 F.2d 530, 533-34 (7th Cir. 1968) ("[U]se of the stolen documents renders the Commission's order unenforceable.").

vi. Improper Cost-Benefit Analysis

Section 5(n) requires evidence-based cost-benefit analysis before liability may be imposed, *see* 15 U.S.C. § 45(n), which the Commission failed to do, relying almost exclusively on Dr. Hill's testimony and Report, *see* Op. 26-28, which does not address LabMD's data security after July 2010, ID 87 n.45. Dr. Hill also ignored or discounted time-related costs. *Compare* Tr. 136:20-21, 200:12-202:11, *with* Op. 28 ("time of trained IT staff can amount to a real cost"). For instance, Dr. Hill did not address time costs associated with file integrity monitoring and penetration tests. Likewise, the Opinion ignored the time costs associated with the various software tools, hardware

devices, and training the Commission claims LabMD should have deployed, as well as the costs associated with remedies, investigation, and enforcement associated with the FTC's attempt to regulate LabMD's practices—costs the FTC itself has said are relevant. *See* Unfairness Statement, 1984 FTC LEXIS 2, *309 ("The Commission also takes account of the various costs that a remedy would entail."). Nor did the Opinion quantify the abstract, intangible, and speculative harms purportedly resulting from LabMD's data security so that they could be compared against the countervailing benefits. *Cf.* Tr. 954-964 (societal benefits of LabMD services).

The Opinion also disregarded LabMD's expenditures on data security. *See, e.g.*, CX0448 at 1 ("[O]ver the past three years, LabMD has spent approximately $230,000 on system upgrades and outside [data-security] vendors…."); RX0412 (LabMD data-security expenditures); Martin Dep. 130-40 (LabMD expenditures on custom Websense security); CX0194; CX0195. Dr. Hill's speculation cannot support the Opinion's flawed Section 5(n) cost-benefit analysis. *See* Dissenting Statement of Commissioner Joshua D. Wright, *In the Matter of Apple, Inc.*, FTC File No. 1123108, 10-16 (Jan. 15, 2014). Again, Complaint Counsel did not meet its burden of proof.[27]

vii. **Commission Final Order is Unlawful and Unenforceable**

The Order is unlawful for several reasons.[28] To begin, the Order exceeds the Commission's authority. The Order does not direct LabMD to "cease and desist" from doing anything, instead

[27] Complaint Counsel did not brief or offer any evidence on this issue. *See* CCAB 1 n.1; RFF 111, ¶495.

[28] The entire Order contains "fencing-in" relief unrelated to LabMD's long-discontinued data-security practices. *See* Op. 36 ("A reasonable and appropriate information program for LabMD's current operations with a computer that is shut down and not connected to the Internet *will undoubtedly differ from an appropriate comprehensive information security program if LabMD resumes more active operations*." (emphasis added)). Three factors are relevant to whether "fencing in" relief is appropriate: "(1) the seriousness and deliberateness of the violation; (2) the ease with which the violation may be transferred to other products; and (3) whether the respondent has a history of prior violations[.]" *In re Telebrands Corp.*, 140 F.T.C. 278, 334, 2005 FTC LEXIS 178, *92 (2005). The Commission did not consider any. None are met here.

ordering LabMD to perform a variety of affirmative tasks (including research projects) unrelated to LabMD's alleged data-security practices more than six years ago, long-since discontinued. Had the Commission brought an action against LabMD in federal district court pursuant to Section 13(b), 15 U.S.C. § 53(b), of the Act, additional remedies may have been available.[29] Instead, the Commission chose to proceed through its in-house administrative process in which the sole available remedy is a cease-and-desist order. *See* 15 U.S.C. § 45(b).

Moreover, Parts I and III of the Order, which require Respondent to, among other things, establish a "comprehensive information security program," conduct research, and disseminate FTC-approved letters at substantial expense are also unlawfully overbroad and "too vague and indefinite to warrant enforcement." *Libbey-Owens-Ford Glass Co. v. FTC*, 352 F.2d 415, 418 (6th Cir. 1965); *see, e.g.*, *Standard Oil Co. v. FTC*, 577 F.2d 653, 661-63 (9th Cir. 1978).

Further, Part III of the Order is invalid because the Commission lacks authority to require LabMD to afford any redress to identifiable "consumers" it believes may have been injured. *See Heater v. FTC*, 503 F.2d 321, 323-27 (9th Cir. 1974). The Commission acknowledges that LabMD was subject to HIPAA in 2008, Op. 12 & n.22, and "this type of notice … [was] required under HIPAA … [after] 2010," Op. 35.[30] The Commission cannot force LabMD to retroactively comply

---

[29] The Commission chose to bring an administrative enforcement action and is limited to remedies available therein. *Cf. FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1027-28 (7th Cir. 1988); FTC Operating Manual, Ch. 11, p. 23 ("Preliminary injunctive relief is appropriate where the challenged practices are immediately and clearly harmful; novel issues of law and remedy should generally be left for administrative proceedings."). Tellingly, the Commission solely cites to actions brought under Section 13(b) in federal district court as precedent for all parts of the Order. *See* Op. 35. It does not cite a single Part 3 adjudication, in which only a "cease and desist" order is available. *See* 15 U.S.C. § 45(b).

[30] HITECH was not enacted until 2009, and HHS did not promulgate its *interim* Breach Notification Rule until August 2009. *See* 74 Fed. Reg. 42,740 (Aug. 24, 2009). Further, the Commission previously stated in this case that the Complaint "does not allege violations of the FTC's Health Breach Notification Rule." January 16 Order at 12 n.20.

with HIPAA (and HITECH) breach notification obligations that were not even in effect when the 1718 File was stolen by Tiversa, particularly because it previously stated that "[t]he Commission does not enforce HIPAA or HITECH," January 16 Order at 12 n.19, and HHS in any event concluded that LabMD had no duty to notify under HITECH, *see* RFF 70, ¶ 303; RX659.

Finally, the Order is invalid because it relates to alleged acts or practices that occurred six to ten years ago, long-since discontinued, where there is no evidence suggesting such alleged practices will recur.[31] *See, e.g.*, *New Standard Pub. Co. v. FTC*, 194 F.2d 181, 183 (4th Cir. 1952); *FTC v. Civil Service Training Bureau, Inc*., 79 F.2d 113, 115-16 (6th Cir. 1935) ("The commission is not authorized to issue a cease and desist order as to practices long discontinued, and as to which there is no reason to apprehend renewal.").

The Commission Opinion addresses LabMD's alleged data-security practices during the Relevant Time Period when LabMD was operational (between January 2005 and July 2010). *See* Op. 11-16. Accordingly, the Commission Opinion properly describes LabMD's alleged data-security practices in the past tense. *See, e.g.*, Op. 16. Complaint Counsel's sole expert on "reasonable" data security, Dr. Raquel Hill (who was told to assume likelihood of substantial harm by Complaint Counsel, RFF 75, ¶¶ 327-329), did not even offer an opinion on LabMD's data security after July 2010. ID 87 n.45. Tiversa stole the 1718 File in or about February 2008, and its alleged "exposure" on LimeWire ended no later than May 2008 even according to the Complaint. *See* Compl. ¶ 20 ("Respondent…removed…[LimeWire] in May 2008, after receiving notice."). The sole basis for the Commission finding that LabMD's data-security practices "causes or is likely to cause substantial injury," 15 U.S.C. § 45(n)—the alleged "availability" of the 1718

[31] *See generally FTC v. Ruberoid Co*., 343 U.S. 470, 473 (1952) (FTC "Orders…not intended to…exact compensatory damages for past acts, but to prevent illegal practices in the future.").

File on LimeWire—ended no later than May 2008. *Cf.* Op. 16-25. LabMD's alleged practices from six or eight years ago cannot justify an Order. *Cf.* Daugherty Decl. ¶¶ 9-19.

viii. **Unlawful Issuance of Complaint**

The Commission's investigation and *issuance* of the administrative Complaint to punish LabMD's CEO for speaking out[32] is also unconstitutional, and thus not in the public interest, as required by 15 U.S.C. §45(b): the First Amendment bars the FTC from retaliating against LabMD for publicly criticizing the FTC. *See Trudeau v. FTC*, 456 F.3d 178, 190 n.22 (D.C. Cir. 2006); *see also FTC v. Klesner*, 280 U.S. 19, 30 (1929).

ix. **Commission Part 3 Administrative Process Violates Due Process**

The Commission Part 3 administrative process violates due process because, as experience has demonstrated, the combination of investigative, prosecutorial, and adjudicative functions within *this* administrative body creates (at least the appearance of) an institutional bias against respondents. Here, consistent with the Commission's pattern and practice over more than twenty years, the Commission found in favor of Complaint Counsel, reversing the Initial Decision dismissing the Complaint. As a former FTC Commissioner observed, the fact that no respondent has prevailed before the Commission—even where, as here, the Initial Decision dismisses the Complaint—for more than twenty years "is a strong sign of an unhealthy and biased institutional process." Joshua Wright, Commissioner, FTC, Section 5 Revisited, 6 (Feb. 26, 2015). *Cf.* ID 4 & nn.1-2 (Commission Rules for deciding dispositive motions). Therefore, under "the special facts and circumstances" present in the FTC and this case, "the risk of unfairness is intolerably high"

[32] *LabMD, Inc. v. FTC*, 776 F.3d 1275, 1277 (11th Cir. 2015) (retaliatory timing of FTC staff decision to recommend Complaint); CX0679 ¶¶ 35-38, 53; LabMD MSD Reply, Ex. 1, 25-28.

and violates due process. *Withrow v. Larkin*, 421 U.S. 35, 58 (1975); *see Williams v. Pa.*, No. 15-5040, 2016 U.S. LEXIS 3774, *12-26 (2016).

B. IRREPARABLE HARM TO RESPONDENT ABSENT STAY

LabMD will suffer irreparable harm absent a stay for at least three reasons.

1. Unpayable and Irrecoverable Compliance Costs

First, the cost of complying with a cease-and-desist order is irreparable harm because that cost is unrecoverable should the respondent prevail on appeal. *In the Matter of Novartis*, 1999 FTC LEXIS 211, at *5-6 (unrecoverable compliance costs are irreparable injury); *In re Toys "R" Us*, 126 F.T.C. 695, 1998 FTC LEXIS 224, *9 (Dec. 1, 1998). Here, absent a stay, LabMD will be forced either to incur substantial unrecoverable compliance costs or to face the possibility of civil penalties.[33] That is irreparable harm. *See, e.g., America's Health Ins. Plans v. Hudgens*, 915 F. Supp. 2d 1340, 1364-65 (N.D. Ga. 2012).

Specifically, the Order requires LabMD to pay for third-party data-security assessments, notices to thousands of individuals and their health insurance companies, and a toll-free telephone number, as well prepare detailed reports for the FTC. Daugherty Decl. ¶¶ 22-25; *see* Order, Pts. I-III. These requirements thus mandate that, prior to any judicial review of the Order, LabMD incur substantial monetary compliance costs (which may be more than $ 250,000.00), which costs LabMD has no ability to pay and in any event would be unrecoverable due to the FTC's sovereign immunity. Daugherty Decl. ¶¶ 3-8, 22-23. Further, the Order requires LabMD to devote substantial time and attention to the variety of tasks it affirmatively requires LabMD to perform, including mailing letters, conducting research, preparing numerous written reports, and interacting

[33] *See* 15 U.S.C. § 45(l)-(m); 81 Fed. Reg. 42,476 (June 30, 2016) ($40,000 penalty for violation of Order).

with (and paying) third-party contractors; LabMD, however, has no personnel who can perform such tasks and no funds with which to hire such personnel. Daugherty Decl. ¶¶ 3-8, 23; *see* Order, Pts. I-VII. And even if it did have or could hire such personnel, LabMD also cannot recover for its personnel's time and effort complying with an Order, even if a U.S. Court of Appeals sets aside the Order *in toto*. This constitutes irreparable harm. *See Bonnette v. D.C. Court of Appeals*, 796 F. Supp. 2d 164, 187 (D.D.C. 2011) (wasted time and effort can be irreparable harm).

2. Violations of Constitutional Rights

Second, the Order violates LabMD's due process, free speech, and associational rights. Violation of constitutional rights is also irreparable harm. *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (holding that deprivation of constitutional rights "unquestionably constitutes irreparable harm"); *see, e.g., Bray v. City of New York*, 04 Civ. 8255 (WHP), 2005 U.S. Dist. LEXIS 21748, *26 (S.D.N.Y. Sept. 30, 2005); *see also De Leon v. Perry*, 975 F. Supp. 2d 632, 663 (W.D. Tex. 2014).

Absent a stay, the Final Order will violate LabMD's procedural due process rights by permanently depriving LabMD of property before LabMD has had an opportunity to be heard at a meaningful time in a meaningful manner. *See Armstrong v. Manzo*, 380 U.S. 545, 552 (1965). To determine whether this due process requirement has been met, courts balance three factors. *See Mathews v. Eldridge*, 424 U.S. 319, 335 (1976) (listing factors). Here, application of the *Matthews* factors confirms that unless the Order is stayed, due process will be violated.

First, as explained above, absent a stay, LabMD will be permanently deprived of, *inter alia*, a substantial sum of money without independent Article III judicial review. Daugherty Decl. ¶¶ 22-23.

Second, the risk that the Commission Opinion and Final Order in this case are in error is high, as explained above and underscored by the Initial Decision dismissing the Complaint, which the Commission reversed. *Cf. Schering-Plough*, 402 F.3d at 1062-63. Further, according to former Commissioner Wright: "[I]n the past nearly twenty years[,] … in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ruled found no liability, the Commission reversed." Wright, Section 5 Revisited at 6. *Compare LabMD, Inc. v. FTC*, 2014 U.S. Dist. LEXIS 65090, at *16 n.6 ("The Court believes that the likelihood of a favorable jurisdictional or merits outcome for LabMD [before the Commission] is slight…."), *with Schering-Plough*, 402 F.3d at 1065 ("It would seem as though the Commission clearly made its decision [to rule against Respondent] before it considered any contrary conclusion.").

Third, staying the effective date the Order would not impose any additional fiscal or administrative burdens, as LabMD has a right to file a petition for review in a U.S. Court of Appeals and be heard on the merits. 15 U.S.C. § 45(c)-(d). Therefore, unless the Order is stayed, LabMD's procedural due process rights will be violated, irreparably harming LabMD.

Parts I and III of the Order will also irreparably harm LabMD by violating its due process right to fair notice, as both are unconstitutionally vague. *See Ga. Pac. Corp.*, 25 F.3d at 1005-06. Given the "severity of possible penalties … for violations," orders must be, "at the outset, sufficiently clear and precise to avoid raising serious questions as to their meaning and application." *FTC v. Henry Broch & Co.*, 368 U.S. 360, 367-68 (1962). Each violation of an effective Commission Order may result in a $40,000 civil penalty. *See* 15 U.S.C. § 45(l)-(m); 81 Fed. Reg. 42,476 (June 30, 2016). Therefore, "the language of its prohibitions should be clear and

precise in order that they may be understood by those against whom they are directed." *FTC v. Cement Institute*, 333 U.S. 683, 726 (1948).

The Final Order fails this test. For instance, it defines "Affected Individual" to "mean any consumer whose personal information LabMD *has reason to believe* was, or *could have been, accessible to unauthorized persons* before July 28, 2016, including, *but not limited to*, consumers listed in the Insurance File…." Order, Definitions § 3 (emphasis added). In turn, Part III requires LabMD send notification letters to all "Affected Individuals." *See* Order, Pt. III. LabMD does not know what this means and how LabMD is supposed to determine compliance. *See* Daugherty Decl. ¶ 22.c.iv.

Part I is also unconstitutionally vague. It requires LabMD to "establish and implement … a comprehensive information security program that is reasonably designed…." Order, Pt. 1. The Commission Opinion implicitly acknowledges Part I's vagueness, suggesting such problems are cured because LabMD may look outside its four corners for further guidance.[34] *See* Op. 34; *see also* IPH Tr. 20:15-17. A central issue in this case is whether the FTC's failure to state with ascertainable certainty at any point what data security practices it believes Section 5 to prohibit or to require violates due process facially and as applied to LabMD for failure to give fair notice. *See, e.g.,* January 16 Order at 14-17; May 19 Order at 9-10; Op. 5-6, 28-31. LabMD still does not know what the FTC thinks (or may later claim) a "reasonably designed" "comprehensive information security program" is and what "administrative, technical, and physical safeguards" the FTC believes now (or may later claim) "appropriate to respondent's size and complexity, the

[34] The Opinion directs LabMD to consult HIPAA for "guidance about comprehensive information security programs." Op. 34. But the Commission previously stated that LabMD is not accused of violating HIPAA and that HIPAA standards are irrelevant. May 19 Order at 4-6. The Commission also previously stated that HIPAA compliance does not preclude liability under Section 5. *See, e.g.,* May 19 Order at 5; January 16 Order at 10-12.

nature and scope of respondent's activities, and the sensitivity of the personal information[.]" Daugherty Decl. ¶ 22.a. *Cf.* Compl. ¶ 10; LabMD MTD at 6-8, 22-28.

Relatedly, Parts I and III are "so standardless that … [they] authorize[] or encourage[] seriously discriminatory enforcement.'" *FCC v. Fox TV Stations, Inc*., 132 S. Ct. at 2317; *see also Giaccio*, 382 U.S. at 402-03. Given circumstantial evidence that FTC staff retaliated against LabMD for publicly criticizing FTC staff, LabMD's fear of discriminatory enforcement is not speculative.[35]

Absent a stay, LabMD's First Amendment rights will also be violated. Part III of the Final Order compels LabMD to affirmatively disseminate FTC-mandated-and-approved letters (the content of which LabMD disagrees with).[36] Such compelled speech irreparably harms LabMD by violating its First Amendment rights. *See International Dairy Foods Ass'n v. Amestoy*, 92 F.3d 67, 72 (2d Cir. 1996).

3. Reputational Harm

Third, reputational harm is also sufficient to support a stay. *See, e.g., Housworth v. Glisson*, 485 F. Supp. 29, 35-36 (N.D. Ga. 1978). Here, the Order requires LabMD to disseminate Commission-approved letters to thousands of individuals and business entities. Daugherty Decl. ¶¶ 24-26. This is irreparable harm.

---

[35] *See supra* Section III.A.2.viii.

[36] For example, whether the factual circumstances under which Tiversa obtained the 1718 File can be accurately described as an "unauthorized disclosure" and "approximate time period" remain disputed.

C. HARM TO OTHER PARTIES AND PUBLIC INTEREST

Because Complaint Counsel is supposed to represent the public interest, the final stay factors—whether a stay will harm other parties and is in the public interest—merge. *North Carolina Board of Dental Examiners*, Dkt. No. 9343, at 3 (Feb. 10, 2012).

The balance-of-harms stay factor favors LabMD. Here, the Initial Decision found that "[t]he record in this case contains no evidence that any consumer … has suffered any harm[.]" ID 52. There is no evidence that anyone has suffered actual identity theft or physical harm as a result of LabMD's allegedly "unreasonable" practices or Tiversa's theft. *Cf.* Op. 15 ("[W]e do not know whether" events relating to 1718 File "resulted in actual identity theft, medical identity theft, or physical harm to any of the consumers[.]"). "[T]he absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years," ID at 52, demonstrates that no parties will be harmed by a stay.[37] Moreover, LabMD is no longer in business, and its computer networks are not connected to the Internet.[38] Daugherty Decl. ¶¶ 4-20; *see also* IDF 39; Op. 36.

A stay is also in the public interest. An agency's compliance with its organic statute, the Administrative Procedure Act, and the federal Constitution is always in the public interest. *See Odebrecht Constr. v. Sec'y, Fla. DOT*, 715 F.3d 1268, 1290 (11th Cir. 2013); *KH Outdoor, LLC v. Trussville*, 458 F.3d 1261, 1272-73 (11th Cir. 2006). Here, the Commission Opinion and Final Order violate LabMD's constitutional and statutory rights.

---

[37] The notification requirements set forth in Part III of the Order relate to events in February 2008, FTC staff commenced its investigation in January 2010, the Commission issued its Complaint in August 2013, and the Order was issued in late July 2016. If the FTC believed such notification time-sensitive, it would have brought an action in federal district court under 15 U.S.C. § 53(b) seeking preliminary injunctive relief.

[38] LabMD's "*computer* security practices…were the sole practices challenged in the Complaint." Op. 25 (emphasis added).

Likewise, the public interest is served by ensuring that the FTC does not extend its power beyond that delegated by Congress. *See, e.g., S. Div. First Premier Bank v. CFPB*, 819 F. Supp. 2d 906, 922 (D.S.D. 2011). Here, a federal judge has found that there is "significant merit" to the argument that the FTC is improperly extending its power in this case. *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7 (N.D.Ga. 2012).

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Application for Stay of Order and ORDER that this matter be stayed pending resolution of LabMD's claims by a U.S. Court of Appeals, or otherwise dismiss this case. Alternatively, the Commission should stay Part III of the Final Order and stay the remainder of the Order for at least sixty (60) days after September 30, 2016, to ensure that a U.S. Court of Appeals has adequate time to rule on a stay motion seeking relief under 15 U.S.C. § 45(g)(2)(B).

Respectfully submitted,

CAUSE OF ACTION INSTITUTE

Patrick J. Massari
Erica L. Marshall
1875 Eye Street, NW
Suite 800
Washington, DC 20006
Tel. (202) 4994232
Fax (202) 338-5842
patrick.massari@causeofaction.org

August 30, 2016

Counsel for Respondent LabMD, Inc.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**DOCKET NO. 9357**
	)	
	)	**PUBLIC**
LabMD, Inc.,	)	
a corporation.	)	
	)	

[PROPOSED] ORDER GRANTING RESPONDENT LabMD, INC.'S APPLICATION FOR STAY OF FINAL ORDER PENDING REVIEW BY A UNITED STATES COURT OF APPEALS

This matter came before the Commission on August 30, 2016, upon an Application for Stay of Final Order Pending Review by a United States court of appeals filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rule 3.56, 16 C.F.R. §3.56, for an Order staying the effective date of the Commission Final Order in the above-captioned action until appellate review, including review by the United States Supreme Court, has concluded.

Having considered this Application and all supporting and opposition papers, and good cause appearing,

IT IS ORDERED that the effective date and enforcement of the Commission's Final Order of July 28, 2016, be stayed upon the filing of a timely petition for review of the Order in an appropriate United States court of appeals pursuant to 15 U.S.C. § 45(c). This stay shall remain effective until the expiration of all periods for petitions for rehearing, rehearing en banc, or certiorari, or until final disposition of all such petitions and any proceedings initiated by a grant of such a petition.

By the Commission.

_____
Donald S. Clark
Secretary

SEAL:

ISSUED:

CERTIFICATE OF SERVICE

I hereby certify that on August 30, 2016, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW, Rm. H-113
Washington, DC 20580

I also certify that I delivered via electronic mail copies of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission 600
Pennsylvania Ave., NW Room CC-8232
Washington, DC 20580

August 30, 2016

Patrick J. Massari

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

August 30, 2016

Patrick J. Massari

EXHIBIT 1

In the Matter of:

LabMD, Inc.

September 16, 2015
Closing Arguments

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

9

1 MS. VANDRUFF: I want to make sure that I
2 understand your question, Your Honor.
3 Your question is whether the procedural posture
4 was that it was filed before discovery had been
5 completed?
6 JUDGE CHAPPELL: My question is, the point that
7 ruling came out, you couldn't possibly have considered
8 anything that came out on the merits in the record, the
9 facts of this case; correct?
10 MS. VANDRUFF: That's correct, Your Honor.
11 And the commission was clear that it was not
12 considering the facts of the case but instead the law to
13 be applied, including the adequacy of notice to
14 respondent and whether the notice that is contained
15 within section 5 of the Federal Trade Commission Act
16 provided sufficient notice to respondent, and the
17 commission held that it did.
18 JUDGE CHAPPELL: So just so I'm clear, the
19 government's position is, a mere breach is all that's
20 required for a section 5 violation.
21 MS. VANDRUFF: Your Honor, the commission in
22 both on its motion to dismiss and --
23 JUDGE CHAPPELL: I'm asking the government's
24 position, not what the commission said.
25 MS. VANDRUFF: Your Honor, a breach is not --

10

1 JUDGE CHAPPELL: We had our own trial here,
2 remember? We were here for a long time. It's been
3 probably over a year.
4 MS. VANDRUFF: I do remember, Your Honor.
5 It's not a matter of whether a mere breach is
6 required because, of course, a breach isn't necessary
7 for there to be a section 5 violation. Rather, what's
8 necessary is that there be an act or practice that
9 causes or is likely to cause consumer injury that
10 consumers cannot reasonably avoid and is not offset by
11 benefits to consumers or competition.
12 JUDGE CHAPPELL: So I think I just heard you,
13 when you said "consumer injury," you're talking about
14 harm or likelihood of harm; correct?
15 MS. VANDRUFF: Correct, Your Honor.
16 JUDGE CHAPPELL: You would concede that that
17 prong is still part of section 5. I mean, I can read
18 it when I look at it, but you would agree that's still
19 part of the what's needed to show a violation; correct?
20 MS. VANDRUFF: Yes, Your Honor.
21 JUDGE CHAPPELL: All right. Thank you.
22 MS. VANDRUFF: Thank you, Your Honor.
23 Your Honor, more than a year ago when the
24 parties delivered their opening statements, Mr. Sherman
25 compared LabMD's business to juggling knives. And

11

1 there's not much that Mr. Sherman and I are likely to
2 agree on today about this case, but, Your Honor,
3 Mr. Sherman's analogy was apt.
4 Running a business that collects hundreds of
5 thousands of consumers' names, dates of birth,
6 Social Security numbers, health insurance information
7 and laboratory test codes and maintains that information
8 electronically is like juggling knives. And when you
9 juggle knives, it's your responsibility to take steps to
10 prevent harm.
11 LabMD had the responsibility to reasonably
12 protect consumers' most sensitive information, but it
13 did not protect that data, and that is why we're here,
14 Your Honor.
15 Hundreds of thousands of consumers, most of
16 whom have probably never heard of LabMD, were and remain
17 powerless to protect themselves and their names, dates
18 of birth, Social Security numbers, health insurance
19 information and laboratory test codes from --
20 JUDGE CHAPPELL: Did you say hundreds of
21 thousands of consumers?
22 MS. VANDRUFF: Yes, Your Honor.
23 JUDGE CHAPPELL: And how many have -- how many
24 came forward? How many have you identified that said
25 they were harmed?

12

1 MS. VANDRUFF: Your Honor, if your question is
2 how many consumers have identified that they were
3 harmed as a proximate cause of LabMD's actions,
4 conduct --
5 JUDGE CHAPPELL: I'm asking you as the person
6 who prosecuted the case.
7 MS. VANDRUFF: Yes, Your Honor.
8 JUDGE CHAPPELL: How many did you bring
9 forward?
10 MS. VANDRUFF: We did not present a consumer
11 witness in this case, Your Honor. But it is undisputed,
12 Your Honor, that there are likely harms resulting from
13 LabMD's failures to reasonably protect the data that it
14 collected and maintained.
15 JUDGE CHAPPELL: I'm not talking about likely
16 right now. I'm talking about actual harm.
17 Did you prove actual harm? And if so, how?
18 MS. VANDRUFF: Your Honor, we -- the actual harm
19 in this case is the release of 9300 consumers' names,
20 Social Security numbers, laboratory test codes, health
21 insurance information, dates of birth.
22 JUDGE CHAPPELL: The release?
23 MS. VANDRUFF: Yes, Your Honor.
24 JUDGE CHAPPELL: Okay. And what evidence do we
25 have of release other than the 1718 File?

13

1 MS. VANDRUFF: That is the evidence of the
2 exposure of information, Your Honor, is the 1718 File
3 that was made available for sharing on the P2P network.
4 That fact has been admitted by LabMD and was in fact
5 downloaded from the P2P network.
6 JUDGE CHAPPELL: So just so I'm clear on the
7 government's position, the fact that the 1718 File
8 alone -- and as you said, that's the one breach you
9 proved -- if that's correct, that's one breach. And
10 even though not one victim has been identified, you're
11 saying that that breach is sufficient harm for a
12 violation of section 5; is that correct?
13 MS. VANDRUFF: Your Honor, 9300 consumers'
14 sensitive information was contained within that file.
15 Those consumers have not been notified of the fact that
16 their information was exposed on the P2P network and
17 therefore have been deprived of the opportunity to take
18 any steps to mitigate harms, for example, by
19 implementing a freeze on their credit.
20 JUDGE CHAPPELL: The government knew who they
21 were; correct?
22 MS. VANDRUFF: Excuse me, Your Honor?
23 JUDGE CHAPPELL: The government knew who these
24 people were. You had the file; correct?
25 MS. VANDRUFF: We had the file, Your Honor,

14

1 that's correct.
2 JUDGE CHAPPELL: Did you undertake to notify
3 anyone?
4 MS. VANDRUFF: We did not undertake to notify
5 consumers, Your Honor.
6 Your Honor, identity thieves value the
7 information that LabMD needlessly exposed for
8 10,000 consumers, and LabMD's failure to implement
9 fundamental, low-cost protections put hundreds of
10 thousands of consumers needlessly at risk.
11 LabMD's blasé approach to data security remains
12 a threat to consumers unless this court enters an order
13 requiring the company to adopt --
14 JUDGE CHAPPELL: Wait, wait, wait, wait. I want
15 to get back to this again.
16 The 1718 File had how many names on it?
17 MS. VANDRUFF: The 1718 File had approximately
18 9300 consumers' names.
19 JUDGE CHAPPELL: 9300. Okay. And that's what
20 you told me earlier that's what you proved.
21 How do you get from 9300 to hundreds of
22 thousands?
23 MS. VANDRUFF: I want -- well, LabMD collected
24 and maintained information regarding 750,000 consumers.
25 JUDGE CHAPPELL: But you just told me earlier

15

1 you proved the one breach, and that was the file that
2 had less than 10,000. But now you're telling me
3 hundreds of thousands. How do you get there?
4 It's simple math I think. 9300 doesn't equal
5 hundreds of thousands.
6 You connected 9300 to a breach.
7 MS. VANDRUFF: Yes, Your Honor.
8 JUDGE CHAPPELL: Now you're jumping to hundreds
9 of thousands.
10 MS. VANDRUFF: I didn't jump, Your Honor. I
11 believe my statement was that LabMD exposed information
12 for 10,000 consumers, so I want to make sure that I'm
13 answering your question, Your Honor.
14 JUDGE CHAPPELL: I've heard "hundreds of
15 thousands" more than once.
16 MS. VANDRUFF: That's true, Your Honor. And
17 that relates to the failure of LabMD to --
18 JUDGE CHAPPELL: No, no, no. You said they were
19 exposed. Where's the evidence they were exposed?
20 MS. VANDRUFF: Your Honor, if that was my
21 statement, it was a misstatement.
22 JUDGE CHAPPELL: Thank you.
23 MS. VANDRUFF: Thank you, Your Honor.
24 My statement was that LabMD needlessly exposed
25 sensitive personal information for approximately

16

1 10,000 consumers.
2 JUDGE CHAPPELL: Thank you.
3 MS. VANDRUFF: Nonetheless, 750,000 consumers'
4 personal information is maintained by LabMD, so I just
5 want to be clear about the factual record in this case,
6 Your Honor.
7 JUDGE CHAPPELL: But that's what I'm trying to
8 maintain here, is the factual record.
9 MS. VANDRUFF: Yes, Your Honor.
10 JUDGE CHAPPELL: I understand 750,000 is the
11 number that were maintained.
12 MS. VANDRUFF: Yes, Your Honor.
13 JUDGE CHAPPELL: But based on what I've heard
14 and read and what you said, we've got a proven exposure,
15 to the extent it's proven, of about 9300.
16 MS. VANDRUFF: Well, Your Honor, again, just
17 turning to the commission's motion -- order on the
18 motion to dismiss --
19 JUDGE CHAPPELL: And again, that order that was
20 issued before the trial on the merits and before all the
21 facts and before we had a record; correct?
22 MS. VANDRUFF: Yes, Your Honor.
23 JUDGE CHAPPELL: All right. Go ahead.
24 MS. VANDRUFF: And that order held that a risk
25 of significant injury would be sufficient to establish

EXHIBIT 2

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
05 06 2014
569773
SECRETARY

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S
PRE-TRIAL BRIEF

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown
Counsel Supporting the Complaint

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580

Exhibit 2

27. Peter Sandrev, Broadvox employee, Cypress Communications, LLC ("Cypress") designee

Cypress Communications provided technology services to LabMD starting in approximately 2004 through March or April 2012. CX0729 (Sandrev, Cypress Comm. Designee, Dep. Tr.) at 13, 19. Before 2009, Cypress provided LabMD with telephone services and broadband internet services. *Id.* at 26. LabMD switched to Voice Over IP Protocol (VOIP) telephony in 2009, *id.* at 13, while continuing its broadband internet service. *Id.* at 26. Cypress did not provide security or other services within LabMD's network. *Id.* at 51, 60-61.

<u>Other Individuals and Entities</u>

28. Robert Boback, Chief Executive Officer of Tiversa Holding Corporation ("Tiversa"), Tiversa designee

Mr. Boback is CEO of Tiversa. CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 11. Tiversa provides information security services, such as breach detection and remediation. *Id.* at 10. Tiversa specializes in finding breaches on peer-to-peer networks. *Id.* at 10-11. In February 2008, Tiversa found and downloaded a file containing information from LabMD ("the 1718 file"). *Id.* at 24-25. In 2008, Tiversa reached out to LabMD regarding its discovery of the 1718 file. *Id.* at 77-78. Tiversa downloaded the 1718 file on three more occasions (*id.* at 57, 63), and it found the file "in multiple locations" as recently as November 2013. *Id.* at 9-10.

29. Erick Garcia

Mr. Garcia was arrested by the Sacramento police on October 5, 2012. CX0720 (Jestes Dep. Tr.) at 25. At that time, he was found to be in possession of LabMD documents. *Id.* at 23. He pled "no contest" to California state charges of identity theft. *Id.* at 44.

EXHIBIT 3

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
12 22 2015
580407
SECRETARY
ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S APPEAL BRIEF

Alain Sheer
Laura Riposo VanDruff
Jarad Brown
Ryan Mehm
Megan Cox

Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Ave., N.W.
CC-8232
Washington, DC 20580
Telephone: (202) 326-2999
Facsimile: (202) 326-3062

Complaint Counsel

TABLE OF CONTENTS

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

RECORD REFERENCE ABBREVIATIONS vi

I. INTRODUCTION 1

II. SUMMARY OF FACTS 1

III. SUMMARY OF ARGUMENT 5

A. A Significant Risk of Concrete Harm Satisfies the Section 5(n) Injury Standard.. 5

B. The Evidence Shows That LabMD's Practices Caused or Were Likely to Cause Substantial Injury 7

IV. PROCEDURAL HISTORY 9

V. QUESTION PRESENTED 10

VI. ARGUMENT 10

A. The Initial Decision is Incorrect as a Matter of Law 11

1. An Act or Practice That Raises a Significant Risk of Concrete Harm Causes Substantial Injury 11

2. Section 5(n) Does Not Require Proof of Known Identity Theft 17

3. Section 5(n) Does Not Require That Substantial Injury Be Established With Mathematical Precision 19

4. Section 5(n)'s Substantial Injury Standard Is Broader Than Article III's Standing Standard 21

B. The Initial Decision is Incorrect as a Matter of Fact 22

1. LabMD's Data Security Practices Created a Significant Risk of Concrete Harm 23

a. LabMD's Data Security Failures Were Multiple, Systemic, and Serious, Placing Consumers at a Significant Risk of Concrete Harm 24

b. The Significant Risk of Concrete Harm Created by LabMD's Data Security Failures Was Magnified When a LabMD Manager Made Sensitive Consumer Data Available for Sharing on the P2P Network 30

i. The Testimony of Professor Shields Demonstrates the Heightened Significant Risk of Concrete Injury Created by LabMD's Sharing of Patient Files on the P2P Network... 32

ii. LabMD's Own Witness Confirmed the Heightened Significant Risk of Concrete Injury Created by LabMD's Sharing of Patient Files on the P2P Network 35

c. The Concrete Harm to Consumers Includes Identity Theft and Medical Identity Theft 35

2. LabMD's Data Security Failures Caused Injury to Consumers Whose Sensitive Personal Information Was Disclosed Without Authorization in the 1718 File 39

VII. CONCLUSION 42

I. INTRODUCTION

LabMD is a multi-million dollar medical testing company that maintains the names, addresses, dates of birth, Social Security numbers, medical diagnoses, financial account information, health insurance information, and financial account information of 750,000 consumers. Despite maintaining consumers' most sensitive personal information, LabMD did not take even the most basic steps to secure it from those who had no right to see it, both within and outside LabMD. LabMD's pervasive security failures caused or were likely to cause substantial consumer injury that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or competition, in violation of the FTC Act's prohibition against unfair practices. 15 U.S.C. § 45(a)(l). The Initial Decision's holding – that Complaint Counsel did not meet its burden of proving that LabMD's practices caused or were likely to cause substantial consumer injury – is in error. Complaint Counsel respectfully requests that the Commission reverse the Initial Decision, review the record *de novo*,[1] find that LabMD violated Section 5 of the FTC Act, and enter the notice order attached.

II. SUMMARY OF FACTS

LabMD conducts laboratory tests on specimen samples from consumers throughout the United States and reports test results to physicians. ID at18-19, ¶¶ 26-29. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35 to $40 million.

---

[1] This brief addresses the Initial Decision, which analyzed only the first prong of Section 5(n)'s Unfairness Test. In addition to proving that LabMD's data security failures harmed consumers, as discussed throughout this brief, Complaint Counsel also proved that consumers could not reasonably avoid the harm that LabMD caused them, CCPTB at 72-73, and that the harm was not offset by countervailing benefits to consumers or competition. CCPTB at 73-75.

EXHIBIT 4

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
02 23 2016
581097
SECRETARY
ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S REPLY BRIEF TO RESPONDENT'S ANSWERING BRIEF

Alain Sheer
Laura Riposo VanDruff
Jarad Brown
Ryan Mehm
Megan Cox

Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Ave., N.W.
CC-8232
Washington, DC 20580
Telephone: (202) 326-2999
Facsimile: (202) 326-3062

Complaint Counsel

B. HIPAA and Other Statutes Do Not Shield LabMD from Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act

Respondent contends that Section 5 cannot be applied to entities in the medical industry, including those subject to HIPAA.[3] *See, e.g.*, RAB at 13-17, 47-48. HIPAA's requirements are irrelevant to this proceeding, a point LabMD conceded in its discovery responses. *See* CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence").

As the Commission has already recognized, there is no separate standard under Section 5 for medical data security. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12; *see also* Comm'n Order Denying Resp't's Mot. for Summ. Decision at 5-6 (May 19, 2014). Courts have upheld Section 5's prohibition of "unfair . . . acts or practices" as a flexible prohibition that applies *across* industries. *See, e.g.*, *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972) (trading stamps); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (televised commercial for shaving cream); *FTC v. Motion Picture Advert. Serv. Co.*, 344 U.S. 392 (1953) (unfair methods of competition in exclusive film-screening agreements); *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010) (online check-processing); *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) (online sale of phone records). Regardless of the industry in which a company operates, the Commission assesses whether a company's data security measures cause or are

[3] Respondent's reference to Mr. Sheer's opening statement for the proposition that the FTC case is based on a "HIPAA statutory standard which was applicable to the LabMD medical data security practices," *see* RAB at 14-15, strains credulity. Mr. Sheer unambiguously stated in his opening that "[t]he evidence will show that LabMD's security practices were unfair under section 5 of the FTC Act." Tr. 11.

EXHIBIT 5

PUBLIC

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
05 07 2014
569816
SECRETARY

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S SEPARATE AND CONCISE STATEMENT OF MATERIAL FACTS AS TO WHICH THERE EXIST GENUINE ISSUES FOR TRIAL

Pursuant to Rule 3.24(a)(2) of the Commission's Rules of Practice, 16 C.F.R. § 3.24(a)(2), Complaint Counsel submits the following Separate and Concise Statement of Material Facts as to which there Exist Genuine Issues for Trial ("Separate Statement"). Part I of this submission sets forth those material facts (with citations to supporting admissible evidence) as to which there is a genuine issue. Part II sets forth statements Respondent has characterized as undisputed and Complaint Counsel's responses to the statements.

notify LabMD of its finding the documents, or that the Sacramento Police had any awareness as to LabMD's "duty to notify under HIPAA" and to whom that obligation would relate. *See* Resp. Mot. Summ. Dec. at Ex. 3. The testimony to which Respondent cites has been completely redacted, and no testimony in the following excerpted pages supports Respondent's statement. *Id.*

Even if this contention were undisputed by Complaint Counsel, it is neither relevant nor material to Respondent's request for summary decision. *See Anderson*, 477 U.S. at 248.

7. *LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, In the Matter of LabMD, Inc., FTC Dkt. No. 9357, ("MTD Opp'n") (Nov. 22, 2013) at 22 fn 15. It must comply with HHS's HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations, including HHS's HIPAA Privacy Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000); HHS's HIPAA Security Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003); and HHS's HITECH Breach Notification Rule, 78 Fed. Reg. 5,566 (Jan. 25, 2013).*

Complaint Counsel's Response: Not a statement of fact, not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Respondent cites no evidence to support its assertion that that LabMD is a HIPAA-covered entity that must comply with specific regulations.

Even if undisputed, this assertion is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA, HITECH, or their implementing regulations, and Respondent did not raise HIPAA, HITECH, or their implementing regulations as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

8. *HIPAA's Security Rule establishes substantive data-security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply.*

Complaint Counsel's Response: Not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Respondent cites no evidence to support its assertion that the HIPAA Security Rule has data security standards or that LabMD is a HIPAA-covered entity that must comply with specific data security standards.

Even if characterized as an undisputed fact, the assertion is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to the HIPAA Security Rule, and Respondent did not raise the HIPAA Security Rule as an affirmative defense. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

9. *HHS exclusively enforces HIPAA and HITECH. Order on Mot. to Dismiss, In the Matter of LabMD, Inc., FTC Dkt. No. 9357, ("MTD Order")(Jan. 16, 2014), at 12 & n.19 ("[T]he Commission cannot enforce HIPAA and does not seek to do so. … The Commission does not enforce HIPAA or HITECH….").*

Complaint Counsel's Response: Not a statement of fact, not supported by evidence, and irrelevant and immaterial.

This statement is a legal conclusion. Whether HHS exclusively enforces HIPAA and HITECH is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA or HITECH, and Respondent did not raise HIPAA or HITECH as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

10. *The FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations. Compl. ¶¶ 22-23; Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., FTC Dkt. No. 9357, 22:10-13 (Sept. 25, 2013) ("Trans."); MTD Order at 12 n. 20 (Jan. 16, 2014); Complaint Counsel's Resp. to LabMD's RFAs, ("CC's RFA Responses") at 8-9 ¶ 7-8, attached hereto as Exh. 4.*

Complaint Counsel's Response: Irrelevant and immaterial.

This contention is irrelevant and immaterial to Respondent's request for summary decision. The Complaint alleges that LabMD's conduct violated Section 5 of the FTC Act and does not contain any allegations of law or fact relating to HIPAA, HITECH, or their implementing regulations, and Respondent did not raise HIPAA, HITECH, or their implementing regulations as an affirmative defense in its Answer. *See* Ans. at 6-7; *Anderson*, 477 U.S. at 248.

11. *The FTC has never specified what data security standards were in place at any given point during the relevant time period or when LabMD specifically violated them.*

Complaint Counsel's Response: Not supported by evidence, irrelevant and immaterial.

Complaint Counsel disputes this contention. The Commission "has repeatedly affirmed its authority to take action against unreasonable data security measures as 'unfair . . . acts or practices' in violation of Section 5." MTD Order at 8. Complaint Counsel sets forth in ¶¶ 1 through 18 of Part I of this statement the disputed facts Complaint Counsel intends to establish at trial to show that LabMD failed to provide reasonable data security.

Even if undisputed, which it is not, this contention does not support Respondent's request for summary decision, as it is irrelevant and immaterial. *See Anderson*, 477 U.S. at 248.

EXHIBIT 6

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**
	)	

OPINION OF THE COMMISSION

By Chairwoman Edith Ramirez, for the Commission:

This case concerns the alleged failure by Respondent LabMD, Inc. to protect the sensitive personal information, including medical information, of consumers whose physicians had entrusted that information to the company. Specifically, Complaint Counsel alleges that LabMD failed to implement reasonable security measures to protect the sensitive consumer information on its computer network and therefore that its data security practices were unfair under Section 5 of the Federal Trade Commission Act. The Administrative Law Judge dismissed the Complaint following an administrative trial, holding that Complaint Counsel had not shown that LabMD's data security practices either caused or were likely to cause substantial injury.

As we explain below, we conclude that the ALJ applied the wrong legal standard for unfairness. We also find that LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system. Among other things, it failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees; and never deleted any of the consumer data it had collected. These failures resulted in the installation of file-sharing software that exposed the medical and other sensitive personal information of 9,300 consumers on a peer-to-peer network accessible by millions of users. LabMD then left it there, freely available, for 11 months, leading to the unauthorized disclosure of the information.

We therefore reverse the ALJ's decision and conclude that LabMD's data security practices constitute an unfair act or practice within the meaning of Section 5 of the FTC Act. We enter an order requiring that LabMD notify affected consumers, establish a comprehensive information security program reasonably designed to protect the security and confidentiality of the personal consumer information in its possession, and obtain independent assessments regarding its implementation of the program.

FACTUAL BACKGROUND

From 2001 until early 2014, LabMD operated as a clinical laboratory conducting tests on patient specimen samples and reporting the test results to its physician customers.[1] Once patients' personal information had been downloaded to LabMD's network, physician-clients could order tests and access test results using LabMD's online portal. IDF 46, 50. Over the course of its operations, LabMD collected sensitive personal information, including medical information, for over 750,000 patients. IDF 42-43. This information included names, addresses, dates of birth, Social Security numbers, insurance information, diagnosis codes, and physician orders for tests and services. IDF 44. In many instances, LabMD retrieved the personal information of all of the patients in its physician-clients' databases, regardless of whether LabMD performed tests for those patients. IDF 43.

As discussed in more detail below, from at least 2005 until 2010, LabMD did not have basic data security practices in place for its network. For instance, it had no file integrity monitoring or intrusion detection system in place and did not adequately monitor traffic coming across its firewalls. It failed to provide data security training to its information technology personnel or other employees, in violation of its own internal compliance program. LabMD also lacked a policy requiring strong passwords. For example, at least six employees used "labmd" as their login password.[2] It also failed to take steps to update its software and protect against known vulnerabilities that could be exploited to gain unauthorized access to consumers' personal information.[3]

Additionally, until at least the fall of 2009, management employees were given administrative rights over their workstations and sales employees had administrative rights over their laptop computers. This gave them the ability to change security settings and to download software applications and files of all types from the Internet, many of which – like peer-to-peer ("P2P") file-sharing applications and music files – were unrelated to LabMD's business.

In or about 2005, the P2P file-sharing program LimeWire was downloaded and installed on a computer used by LabMD's billing manager.[4] It was widely known in the billing

[1] IDF 24-26. This opinion uses the following abbreviations for citations to the record:

Comp.: Complaint
ID: Initial Decision of the Administrative Law Judge
IDF: Numbered Findings of Fact in the ALJ's Initial Decision
Tr.: Transcript of Trial before the ALJ
CX: Complaint Counsel's Exhibit
RX: Respondent's Exhibit
RAB: Respondent LabMD Inc.'s Corrected Answering Brief
Motion to Dismiss: Respondent LabMD Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings (Nov. 12, 2013)

[2] CX0167; CX0705-A (Bradley dep.) at 125-26.

[3] *See, e.g.*, CX0740 (Hill Expert Report) ¶¶ 70-71, 98-99; CX0731 (Truett dep.) at 81-84.

[4] *See, e.g.*, CX0755 at 4, Response to Interrog. 3; CX0766 at 8-9, Admiss. 40-41; CX0447 at 6-7; CX0150 (Screenshot: C:\) at 1; CX0730 (Simmons dep.) at 10, 24-25.

department that the billing manager and others in the department regularly used LimeWire while at work, primarily for downloading and listening to music.[5]

Often used to share music, videos, and photographs, P2P file-sharing applications allow one computer user to search for and download all files that have been made available for sharing on a "host" computer that is also using the same file-sharing application. IDF 63. LimeWire was one of a number of common P2P applications that used the "Gnutella" P2P protocol.[6] A user shares files on the Gnutella network by designating a directory on his or her computer as a shared directory, making all of the files within the directory freely available for downloading and viewing by other users of the network.[7] Once a file is downloaded by a user from the Gnutella network, the file can be shared further without downloading it again from the original computer. Because of the ease of sharing, it can be extremely difficult or impossible to remove a file from the network once it has been downloaded.[8] Between 2005 and 2010, the Gnutella network had between two and five million users online at any given time.[9]

In February 2008, Richard Wallace, a forensic analyst employed by Tiversa Holding Company, a data security company, discovered and downloaded a copy of one of LabMD's insurance aging reports.[10] Mr. Wallace testified that he used a P2P network and standard P2P application like LimeWire to download the file from a LabMD IP address in Atlanta, Georgia. IDF 121-22. This file, dated June 7, 2007 and referred to as the "1718 file," contained 1,718 pages of sensitive personal information for approximately 9,300 consumers, including their names, dates of birth, social security numbers, "CPT" codes designating specific medical tests and procedures for lab tests conducted by LabMD, and, in some instances, health insurance company names, addresses, and policy numbers. IDF 78, 82. Using the "browse host" function on LimeWire, which enabled him to view all of the shared, downloadable files on LabMD's computer, Mr. Wallace downloaded other documents from the same IP address. IDF 127. Three of these documents also contained sensitive personal information from three consumers, including health insurance data, date of birth, and social security number.[11]

In May 2008, Tiversa, with the aim of obtaining LabMD's business, informed LabMD that the 1718 file had been exposed through LimeWire. IDF 128. Tiversa repeatedly solicited LabMD, offering to sell its breach detection services, and later falsely claimed it had evidence that the 1718 file had spread further across P2P networks.[12]

[5] CX0681 at 7; CX0733 (Boyle IH) at 27; CX0730 (Simmons dep.) at 140; CX0716 (Harris dep.) at 86-89, 149; CX0714-A ([Fmr. LabMD Empl.] dep.) at 29-33, 128-31.
[6] IDF 69-71; Shields, Tr. 851.
[7] *See, e.g.*, Shields, Tr. 852; CX0738 (Shields Rebuttal Report) ¶ 17; RX533 (Fisk Expert Report) at 10.
[8] *See, e.g.*, Shields, Tr. 852-54; CX0738 (Shields Rebuttal Report) ¶ 21; CX0740 (Hill Report) ¶ 44.
[9] *See* Fisk, Tr. 1181; RX533 (Fisk Expert Report) at 15; Shields, Tr. 833.
[10] IDF 121-24. Used to track accounts receivable, LabMD's insurance aging reports are spreadsheets documenting insurance claims and payments, and include patients' medical information supporting insurance claims. IDF 52-53.
[11] *Id.*; RX0645 at 39, 42, 43 (*in camera*). We have concentrated our analysis on the much larger 1718 file, but the exposure of sensitive personal information in these additional documents raises concerns similar to those raised by the exposure of comparable information in the 1718 file.
[12] IDF 128-29. In 2009, in response to a request for information from the Commission, a Tiversa affiliate provided the 1718 file to the FTC. IDF 138.

After being contacted by Tiversa, LabMD conducted an internal investigation to determine how the 1718 file had been exposed. IDF 80, 84. It turned out that, during the time that LimeWire had been on the billing manager's computer, the entire contents of her "My Documents" folder had been designated for sharing. IDF 85, 89. Although most of the 950 files in the shared folder were music or videos, the 1718 file and other documents were shared as well. IDF 85-87. Despite clear onscreen warnings from LimeWire that the documents were being shared, neither the billing manager nor anyone else who knew about the P2P file-sharing program did anything to protect the patient information that was being exposed until Tiversa notified LabMD of the disclosure.[13] Once informed of the disclosure, LabMD never notified any of the consumers listed in the 1718 file that their personal information had been disclosed.[14]

Later, in 2010, LabMD hired an independent security firm, ProviDyn, to perform penetration tests on its system and catalogue the vulnerabilities it found. CX0070. ProviDyn identified a number of urgent and critical vulnerabilities on four of the seven servers it tested and rated the overall security of each server as poor. CX0067-CX0071. Among the four servers was the "Mapper" server that LabMD used to receive sensitive information of hundreds of thousands of consumers from physician clients.[15]

Then, in 2012, the Sacramento California Police Department found 40 LabMD "day sheets" containing the names and social security numbers of 600 people, copied checks revealing the names, addresses, and bank numbers of nine individuals, and one money order payable to LabMD (collectively, the "Sacramento documents") while searching the home of individuals suspected of utility billing theft. IDF 182-86, 189-92. The Sacramento Police Department collected the documents as evidence and arrested the two individuals who had possession of the documents; the arrested individuals later pled *nolo contendere* to identity theft. IDF 194-96.

In January 2014, LabMD stopped conducting lab tests and began winding down its business. IDF 36. It continues to preserve tissue samples and provide past test results to healthcare providers. IDF 37, 39. LabMD has not destroyed or deleted any of the patient data it collected. As a result, it continues to maintain the personal data of hundreds of thousands of people on its computer system. IDF 40-42.

PROCEDURAL BACKGROUND

A. The Allegations

On August 28, 2013, the Commission unanimously voted to issue a Complaint against LabMD, alleging that, from 2005 onward, LabMD failed to provide reasonable and appropriate security for personal information stored on its computer network and that its failure caused or

[13] *See* CX0152 (Screenshot: LimeWire: My Shared Files) at 1; CX0154 (Screenshot: LimeWire Get Started) at 1 (screenshots showing warning that the billing computer was sharing numerous files and sub-folders, which could create a security risk); CX0730 (Simmons dep.) at 27-29, 93 (LabMD IT specialist who investigated the 1718 file incident, noting that the billing manager "had no idea what she was doing" when it came to P2P file sharing).
[14] CX0710-A (Daugherty Designee dep.) at 48; Daugherty, Tr. 1087.
[15] CX0725-A (Martin dep.) at 82-83; CX0704-A (Boyle dep.) at 24.

was likely to cause substantial consumer injury, including identity theft, medical identity theft, and other harms, such as the disclosure of sensitive, private medical information. Comp. ¶¶ 10, 12, 22. The Complaint alleges further that LabMD "could have corrected its security failures at relatively low cost using readily available security measures"; that "consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid [these] possible harms"; and that these harms are not offset by countervailing benefits to consumers or competition. *Id.* ¶¶ 11, 12, 22. The Complaint also alleges that LabMD experienced two security breach incidents exposing the 1718 file and possibly other documents containing personal information and the Sacramento documents. *Id.* ¶¶ 17-20. Accordingly, the Complaint alleges that LabMD's security failures constitute an unfair act or practice in violation of Section 5 of the FTC Act, and seeks, among other things, relief requiring LabMD to implement a comprehensive program to protect the security, confidentiality, and integrity of the personal information in its possession. *Id.* ¶¶ 22-23; Comp., Notice Order § I at 7.

LabMD filed its Answer on September 17, 2013. It admitted that LimeWire had been downloaded and installed on a computer used by its billing manager, that it was installed "no later than 2006," and that the 1718 file contains "personal information about approximately 9,300 referring physicians' patients, including names, dates of birth, SSNs, CPT codes, and health insurance company names, addresses, and policy numbers." Ans. ¶¶ 18-19. LabMD denied, or pled insufficient knowledge to admit or deny, most of the other allegations concerning the LimeWire and Sacramento security breach incidents. *Id.* ¶¶ 17-20. LabMD also denied that its security practices were unreasonable or inappropriate and that they violated the FTC Act. Ans. ¶¶ 10, 23.

In addition, LabMD asserted a number of affirmative defenses, including contentions that the Commission lacks statutory authority to regulate the acts or practices alleged in the Complaint; the practices alleged did not cause and are unlikely to cause substantial injury to consumers; and the Commission's alleged failure to provide notice or meaningful standards on data security violates the Fifth Amendment's due process guarantee and the Administrative Procedure Act. *Id.* at 6-7.

B. LabMD's Motions to Dismiss and for Summary Decision

On November 12, 2013, LabMD filed the first of several motions to dismiss the Complaint, arguing that the Commission lacks statutory authority to regulate or bring enforcement actions with respect to data security practices and that the Complaint failed to state a valid claim for relief. The Commission rejected LabMD's jurisdictional arguments and denied the motion on January 16, 2014.[16]

[16] On April 24, 2015, LabMD filed another motion to dismiss, arguing that Complaint Counsel had engaged in "misconduct and indiscretions" in the investigation and prosecution of the case, including its reliance on the evidence provided by Tiversa. The ALJ denied that motion on May 26, 2015. On July 14, 2015, LabMD moved to amend its Answer to add another affirmative defense claiming that the ALJ was not properly appointed under the Appointments Clause of the U.S. Constitution, and then filed another motion to dismiss contending that the FTC's enforcement action was therefore constitutionally defective. The ALJ granted LabMD leave to amend its Answer on July 27, 2015, and we denied the motion to dismiss on September 14, 2015.

On April 21, 2014, LabMD filed a motion for summary decision in which it again raised many of the same jurisdictional challenges and due process arguments it had raised in previous filings. The Commission denied LabMD's motion by order dated May 19, 2014.

C. LabMD's Collateral Attempts to Enjoin the FTC's Enforcement Action

On November 14, 2013, LabMD filed a complaint in the U.S. District Court for the District of Columbia, seeking to enjoin the FTC's enforcement action based on many of the same arguments it had made in its motions to dismiss. A month later, LabMD filed a petition for review in the Eleventh Circuit and moved for a stay of the FTC's administrative proceedings. On February 18, 2014, the Eleventh Circuit dismissed LabMD's petition for lack of jurisdiction. *LabMD, Inc. v. FTC*, Case 13-15267 (11th Cir., Feb. 18, 2014) (*per curiam*). LabMD subsequently withdrew its pending complaint before the D.C. District Court.

In March 2014, LabMD sued for declaratory and injunctive relief in the U.S. District Court for the Northern District of Georgia seeking to enjoin the proceeding before the ALJ and to prohibit the FTC from bringing any further action against it. The district court denied LabMD's motion and granted the FTC's motion to dismiss for lack of subject matter jurisdiction on May 12, 2014. *LabMD, Inc. v. FTC*, 2014 WL 1908716 (N.D. Ga., May 12, 2014). The Eleventh Circuit affirmed on January 20, 2015, concluding that LabMD's arguments are reviewable only after the administrative proceedings are final. *LabMD, Inc. v. FTC*, 776 F.3d 1275, 1277 (11th Cir. 2015).

D. The Evidentiary Hearing

The evidentiary hearing before Chief Administrative Law Judge D. Michael Chappell began on May 20, 2014 and was completed on July 15, 2015.[17]

Complaint Counsel called four expert witnesses. Dr. Raquel Hill, a tenured professor of computer science at Indiana University, was called to assess whether LabMD provided reasonable security for the personal information on its computer networks. Rick Kam, a certified information privacy professional, was asked to assess the risk of injury to consumers resulting from the unauthorized disclosure of sensitive personal information and to describe the types of consumer injuries that occur when firms fail to take reasonable precautions to protect private financial and medical data. James Van Dyke, the founder and President of Javelin Strategy & Research, which conducts survey research on identity theft, assessed the risk of injury to consumers whose personally identifiable information has been disclosed or not adequately protected from unauthorized disclosure. Finally, Dr. Clay Shields, a tenured computer science professor at Georgetown University with special expertise in P2P networks, testified as a rebuttal expert on various issues relating to the functionality of P2P networks and LabMD's exposure of the 1718 file.

[17] Completion of the trial was delayed while Mr. Wallace, the Tiversa forensic analyst who had discovered LabMD's 1718 file, sought to obtain prosecutorial immunity. ID 5.

LabMD called four fact witnesses: Michael J. Daugherty, LabMD's founder and President; Mr. Wallace of Tiversa; Professor Eric Johnson of Dartmouth University, with whom Tiversa shared the 1718 file as part of a research project; and Daniel Kaufman, a deputy director of the FTC's Bureau of Consumer Protection. LabMD also called one expert witness: Adam Fisk, a former lead engineer at LimeWire, who was asked to opine on whether LabMD provided adequate security for the medical information on its computer network.

E. The ALJ's Initial Decision

Judge Chappell issued his Initial Decision on November 13, 2015. He focused on only the first of the unfairness standard's three elements, holding that Complaint Counsel had failed to prove that LabMD's computer data security practices "caused" or were "likely to cause" "substantial consumer injury," as required by Section 5(n) of the FTC Act. On that basis, he dismissed the Complaint.

In so holding, the ALJ defined the phrase "likely to cause" to mean "having a high probability of occurring or being true." ID 54. Applying this standard, the ALJ rejected Complaint Counsel's argument that identity and medical identity theft-related harms were "likely" for consumers whose personal information was maintained on LabMD's computer network. He concluded that, "[a]t best, Complaint Counsel has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm." ID 14.

According to the ALJ, neither the exposure of the 1718 file nor the Sacramento documents incident demonstrated that LabMD's security practices either caused or were likely to cause consumer injury. As to the 1718 file, he rejected Complaint Counsel's argument that the very disclosure of sensitive personal medical information, including lab tests for conditions such as HIV, prostate cancer, and herpes, itself represented substantial consumer injury. He concluded that "[e]ven if there were proof of such harm, this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a 'substantial injury' within the meaning of Section 5(n)." ID 13.

The ALJ also found there was little likelihood of future harm. He explained that Complaint Counsel had not shown that the 1718 file was downloaded by anyone other than Tiversa, and that Tiversa had shared the information only with an academic researcher and the FTC. *See* ID 59-60; IDF 169-81. He concluded that this, combined with the fact that there had been no consumer complaints or injuries linked to the disclosure of the 1718 file, indicated that there was little likelihood that the information in the file would be disclosed to additional individuals or would cause future harm. ID 60.

With respect to the Sacramento incident, the ALJ concluded that Complaint Counsel had failed to establish a causal connection between the incident and any failure of LabMD to reasonably protect data on its computer network as alleged in the Complaint. The ALJ noted that the documents were found in hard copy form and that no evidence had been presented establishing that the documents were maintained on, or taken from, LabMD's computer network. ID 13, 71. Additionally, although the documents were discovered in the possession of identity thieves, the ALJ held that Complaint Counsel had not shown that the exposure of the Sacramento

documents caused or was likely to cause substantial consumer harm. In particular, he highlighted the lack of evidence of consumer complaints or injuries resulting from the incident and reasoned that, because the documents had been booked into evidence by the Sacramento Police Department, there was also no likelihood of future injury. ID 13, 72.

The ALJ declined to address or make any findings of fact with respect to the other issues in the case, including the reasonableness of LabMD's data security practices and the two other unfairness elements – whether the alleged harm was reasonably avoidable by consumers and whether it was outweighed by countervailing benefits to consumers or competition. ID 49, 55-56. He also concluded that, in light of his holding, it was unnecessary to address LabMD's affirmative defenses. ID 14.

Complaint Counsel appeal the ALJ's ruling, arguing that the ALJ misconstrued Section 5(n) by applying an unduly stringent substantial injury standard and failing to recognize that economic and physical harm are not the only forms of cognizable injury. They contend further that he erred by placing undue emphasis on the lack of evidence of particular consumers who suffered actual injury. Complaint Counsel also argue that the ALJ erred by requiring that the probability that consumers will suffer injury be precisely quantified.

LabMD, in turn, urges us to adopt the standard set forth in the ALJ's Initial Decision and affirm his dismissal of the Complaint. As alternative bases for dismissal of the Complaint, LabMD argues that the Commission's unfairness standard is unconstitutionally void for vagueness and fails to provide due process and fair notice. LabMD also claims that dismissal is warranted because the information Complaint Counsel obtained regarding the 1718 file and "all derivative evidence" are based on "unreliable, if not false evidence" provided by Tiversa.

STANDARD OF REVIEW

The Commission reviews the ALJ's findings of fact and conclusions of law *de novo,* considering "such parts of the record as are cited or as may be necessary to resolve the issues presented." 16 C.F.R. §3.54. Our *de novo* review applies to "both findings of fact and inferences drawn from those facts." *McWane, Inc.*, Docket No. 9351, 2014 FTC LEXIS 28, at *30 (Jan. 30, 2014), *aff'd, McWane, Inc. v. FTC*, 783 F.3d 814 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 1432 (2016). We have nonetheless carefully considered the ALJ's factual findings and analysis in the course of conducting our own review.[18]

[18] TechFreedom moved for leave to file an *amicus curiae* brief in support of LabMD. That motion is hereby granted. Most of TechFreedom's arguments are similar to those raised by LabMD, and our discussion of LabMD's arguments incorporates our assessment of TechFreedom's related points. An additional argument TechFreedom raises is that the Commission must defer to the ALJ's Initial Decision absent an abuse of discretion and that the Commission lacks authority to overrule the decision. The contention is meritless. As noted above, the Commission reviews the ALJ's findings *de novo*.

ANALYSIS

I. The Unfairness Standard

Section 5 of the FTC Act authorizes the Commission to challenge "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. §45(a). In 1994, Congress added Section 5(n) to the Act, providing that an act or practice may be deemed unfair if (1) it "causes or is likely to cause substantial injury to consumers"; (2) the injury "is not reasonably avoidable by consumers themselves"; and (3) the injury is "not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). This three-part test, derived from the Commission's 1980 *Policy Statement on Unfairness*,[19] codifies the analytical framework for the Commission's application of its unfairness authority.

Our resolution of this case turns in significant part on the meaning of the first prong of Section 5(n) and the relationships that tie the various elements of the unfairness standard together. In construing and applying Section 5(n), we draw considerable guidance from the *Unfairness Statement* and the many Commission actions and federal court rulings applying the unfairness standard. Within the framework set out by Congress, it is up to the Commission to determine, on a case-by-case basis, which practices should be condemned as "unfair." *See FTC v. Wyndham Worldwide, Inc.*, 799 F.3d 236, 243 (3d Cir. 2015) ("Congress designed the term as a 'flexible concept with evolving content,' and 'intentionally left [its] development . . . to the Commission.'"); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985) (noting the Commission may exercise its discretion to ascertain which "acts or practices . . . injuriously affect the general public" and "to prevent" such acts) (quoting H.R. REP. NO. 75-1613, at 3 (1937)).

The central focus of any inquiry regarding unfairness is consumer injury. *See* FTC, Credit Practices Rule, Statement of Basis and Purpose, 49 Fed. Reg. 7740, 7743 (Mar. 1, 1984) ("*Credit Practices SBP*"), *aff'd*, *Am. Fin. Servs. Ass'n*, 767 F.2d 957. As reflected in the first prong of Section 5(n), a finding of unfairness requires that the injury in question be "substantial." It is well established that substantial injury may be demonstrated by a showing of a small amount of harm to a large number of people, as well as a large amount of harm to a small number of people.[20] Additionally, in the *Unfairness Statement*, the Commission noted that most cases of unfairness involve economic harm or health and safety risks, and that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair." *Unfairness*

[19] *See* FTC, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction ("*Unfairness Statement*") (Dec. 17, 1980) (*appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984)), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; S. REP. NO. 103-130, at 12-13 (1993) ("SENATE REPORT") (explaining that the amendments were "intended to codify . . . the principles of the FTC's [*Unfairness Statement*]" and to "enable the FTC to proceed in its development of the law of unfairness with a firm grounding in the precedents decided under this authority, and consistent with the approach of the FTC and the courts in the past").

[20] *See* SENATE REPORT at 13; *Unfairness Statement*, 104 F.T.C. at 1073 n.12; *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010) (*quoting Am. Fin. Servs. Ass'n*, 767 F.2d at 972); *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988).

Statement, 104 F.T.C. at 1073. The Commission, however, also recognized that, in extreme cases, subjective types of harm might well be considered as the basis for a finding of unfairness, citing as an example "harassing late-night telephone calls" from debt collectors. *Id*. at 1073 n.16; *see also* SENATE REPORT at 13 (legislative history of Section 5(n) referring to "abusive debt collection practices" and "high pressure sales tactics" as examples of contexts in which the unfairness standard may apply). Indeed, neither the *Unfairness Statement* nor Section 5(n) forecloses the possibility that an intangible but very real harm like a privacy harm resulting from the disclosure of sensitive health or medical information may constitute a substantial injury.

The first prong of Section 5(n) also includes a causation requirement that is satisfied where a practice "causes . . . substantial injury." 15 U.S.C. § 45(n). The practice need not be the only or most proximate cause of an injury to meet this test. As the Third Circuit recently explained in *Wyndham*, "that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms." 799 F.3d at 246.

A practice may also meet the first prong of Section 5(n) if it is "likely to cause substantial injury." Congress therefore expressly authorized the Commission to address injuries that have not yet manifested. *Id.* ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."). In determining whether a practice is "likely to cause a substantial injury," we look to the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur. Thus, a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low. For example, in *Philip Morris, Inc.*, 82 F.T.C. 16 (1973), the Commission found unfair the unsolicited distribution of free sample razor blades in a manner that could lead the razors to fall into the hands of small children – even though no child had yet been injured. *See also Int'l Harvester Co.*, 104 F.T.C. at 1064 (failure to include a warning label on a tractor gas cap was unfair where the likelihood of harm was low but the injuries were severe). As is the case for analysis of unfairness generally, this evaluation does not require precise quantification. What is important is obtaining an overall understanding of the level of risk and harm to which consumers are exposed. *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 625 (D. N.J. 2014), *aff'd on other grounds*, 799 F.3d 236 (3d Cir. 2015)*; see also Int'l Harvester Co.*, 104 F.T.C. at 1065 n.59; *Am. Fin. Servs. Ass'n*, 767 F.2d at 986; SENATE REPORT at 13.

Under the second and third prongs of Section 5(n), we ask whether consumers could have reasonably avoided the asserted injury and whether it is outweighed by countervailing benefits. *See Unfairness Statement*, 104 F.T.C. at 1073-74; *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1363-64 (11th Cir. 1988) (Commission's "definition of 'unfairness' focuses upon *unjustified* consumer injury") (emphasis added).

Among the types of acts or practices the Commission has long challenged under its unfairness authority are unreasonable and inappropriate data security practices.[21] The Third

[21] To date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases. *See, e.g.*, Commission Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *CardSystems Solutions, Inc.*, FTC File No. 052-3148, Docket No. C-4168 (2006), *available at* https://www.ftc.gov/enforcement/cases-

Circuit succinctly summarized how the three prongs of the unfairness test apply in the data security context in *Wyndham*, describing it as "a cost-benefit analysis" that "considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." 799 F.3d at 255.

This framework dovetails with the analysis the Commission has consistently employed in its data security actions, which is encapsulated in the concept of "reasonable" data security. As the Commission has explained:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. . . . [T]he Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

Commission Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014) ("50th Settlement Statement"); *see also* Comm'n Order Den. Mot. to Dismiss at 17-19.

Thus, we evaluate whether LabMD's data security practices, taken together, failed to provide reasonable and appropriate security for the sensitive personal information on its computer network, and whether that failure caused or was likely to cause substantial injury that consumers could not have reasonably avoided and that was not outweighed by benefits to consumers or competition.

We now present an overview of LabMD's data security practices and then apply each of the three prongs of Section 5(n) to the facts here.

II. LabMD's Data Security Practices

LabMD was entrusted with patients' sensitive medical and financial information, and was obligated to put reasonable security systems in place to guard against the risk of an unauthorized release of such information. As discussed below, LabMD did not employ basic risk management techniques or safeguards such as automated intrusion detection systems, file integrity monitoring software, or penetration testing. It also failed to monitor traffic coming across its firewalls. In addition, LabMD failed to provide its employees with data security training. And it failed to

proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *Nations Title Agency, Inc.*, FTC File No. 052-3117, Docket No. C-4161 (2006), *available at* https://www.ftc.gov/enforcement/cases-proceedings/052-3117/nations-title-agency-inc-nations-holding-company-christopher; *DSW, Inc.*, 141 F.T.C. 117 (2006); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

adequately limit or monitor employees' access to patients' sensitive information or restrict employee downloads to safeguard the network.

A. LabMD Failed to Protect its Computer Network or Employ Adequate Risk Assessment Tools

Widely known and accepted standards governing minimum reasonable data security practices have long established that risk assessment is an essential starting point. For example, as of 2003, regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat, 1936 (1996), have required covered entities like LabMD that transmit health information to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."[22] While the requirements imposed by HIPAA do not govern whether LabMD met its obligations under Section 5 of the FTC Act, they do provide a useful benchmark for reasonable behavior. Similarly, since at least 2002, National Institute of Science and Technology ("NIST") guidelines provided a framework for risk management for information technology systems that included testing for the presence of vulnerabilities.[23] Additionally, since at least 2005, IT practitioners commonly used intrusion detection systems and file integrity monitoring products to assess whether there were risks on networks.[24] They also used "penetration tests," which are a series of audits that check for conditions such as whether a server's ports are unused and open or whether industry-known software bugs are unpatched, to spot vulnerabilities that criminals could exploit to obtain unauthorized access to sensitive information on the network.[25]

Although LabMD had at least two IT employees on staff,[26] it did none of this. It had no intrusion detection system or file integrity monitoring at all, and it employed penetration testing

[22] 45 C.F.R. 164.308 (a)(1)(ii)(A); *see also* CX0405 (HIPAA Security Series) at 1 ("The Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities."). Throughout this proceeding LabMD has acknowledged that it is subject to HIPAA. *See, e.g.,* Motion to Dismiss at 4 ("LabMD's patient-information data-security practices are, and were at all times relevant, regulated under HIPAA and HITECH.").

[23] *See* CX0400 at 17-18 (NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) (2002)); *see also* National Research Council, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION (1997) ("NRC Report") (cited as a "comprehensive information security program[] concerning electronic health data," CX0740 (Hill Expert Report) ¶ 60 and n.8) (noting that "[o]rganizations should formally assess the security and vulnerabilities of their information systems on an ongoing basis"), *available at* http://www.nap.edu/catalog/5595.html.

[24] CX0740 (Hill Expert Report) ¶¶ 4, 48, 65, 69 n.22, 104(h). Intrusion detection systems analyze large amounts of network traffic and issue alerts and warnings about threats and suspicious activity. *Id.* ¶ 65. File integrity monitoring products identify changes in critical files that may indicate that malware is present on a network. *Id.*

[25] CX0400 at 24-25; CX0740 (Hill Expert Report) ¶¶ 70-72.

[26] *See, e.g.,* CX0707 (Bureau dep.) at 7; CX0717 (Howard dep.) at 7-11; CX0719 (Hyer dep.) at 46-47, 49; CX0735 (Kaloustian IH) at 7, 13-17; CX0724 (Maire dep.) at 10-11; CX0725-A (Martin dep.) at 9-10; CX0730 (Simmons dep.) at 7. LabMD objects to the introduction of testimony by former LabMD IT employee Curt Kaloustian, arguing that his testimony was obtained during an investigational hearing when LabMD counsel was not present and attorney-client privilege may not have been preserved. LabMD does not identify any particular testimony that purportedly reveals privileged information, and we find no factual basis for LabMD's objection. At the outset of the investigational hearing, the FTC investigator explained that he did not want Mr. Kaloustian "to reveal the content of

only after Tiversa had notified it that the 1718 file was available through LimeWire.[27] The tools that LabMD used to help mitigate risk were antivirus programs, firewall logs, and manual computer inspections, which could identify only a limited scope of vulnerabilities and were often used in a manner that further reduced their effectiveness.[28] For example, LabMD did not consistently update virus definitions[29] or run and review scans.[30] Also, LabMD's manual inspections were not used to detect security risks but merely responded to complaints about computer performance.[31]

LabMD also failed to monitor its network for unauthorized intrusions or exfiltration, which is another common practice long employed by IT professionals.[32] LabMD's firewalls were ineffective for the purpose of risk assessment for two reasons. First, they were not configured properly.[33] Second, no one at LabMD reviewed firewall logs or network activity logs except in connection with troubleshooting a problem, such as with Internet speed or connectivity. For example, there was no attempt to monitor outgoing traffic for items like social security numbers.[34]

One significant consequence of these failures by LabMD was that LimeWire ran undetected on the billing manager's computer between 2005 and 2008.[35] File integrity

any communication [he may have] had with an attorney" and offered Mr. Kaloustian the opportunity to proceed only with personal counsel or counsel for LabMD, which Mr. Kaloustian declined. CX0735 (Kaloustian IH) at 9-10. In any event, we rely on Mr. Kaloustian's testimony only for factual descriptions of LabMD's network, equipment, and applications, as well as the day-to-day actions and practices of LabMD's IT employees.

[27] CX0731 (Truett dep.) at 122; CX0717 (Howard dep.) at 58, 140-41; CX0734 (Simmons IH) at 68-69; JX0001-A (Joint Stipulations) at 4; CX0735 (Kaloustian IH) at 92-93.

[28] *See, e.g.*, CX0740 (Hill Expert Report) ¶ 68; CX0735 (Kaloustian IH) at 43-44, 126-27, 187-88.

[29] *See, e.g.*, CX0035 (APT service invoice) at 3; CX0731 (Truett dep.) at 81-84; CX0735 (Kaloustian IH) at 91-92 (many LabMD servers did not receive new virus definitions), 126-32, 160-61 (LabMD relied on individual employees to download new virus definitions from manufacturer websites, but many lacked an internet connection).

[30] LabMD relied on individual employees to run scans, but had no policy requiring them to do so or explaining how and when to conduct the scans. CX0735 (Kaloustian IH) at 126-32. In addition, the Symantec/Norton antivirus program did not automatically report the results of scans to LabMD's IT employees. CX0717 (Howard dep.) at 63-64, 70-71. Thus, LabMD's programs were incapable of determining and revealing whether new viruses had infected the servers and computers. *See* CX0731 (Truett dep.) at 83-84; CX0717 (Howard dep.) at 64-66.

[31] CX0730 (Simmons dep.) at 104, 143-45; CX0707 (Bureau dep.) at 50-51, 89-90.

[32] CX0740 (Hill Expert Report) ¶¶ 65, 68-69(b). This dovetails with HIPAA's requirement that covered entities "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 45 C.F.R. § 164.308(a)(1)(ii)(D).

[33] Although properly configured firewalls should be in place at the network gateway *and* on employee workstations, CX0740 (Hill Expert Report) ¶¶ 31(c), 104(g), until the middle of 2010, LabMD relied only on a ZyWall firewall at the network level. CX0731 (Truett dep.) at 65. The type of network traffic information the ZyWall firewall could record and store was limited, and it could only log information for a few days of traffic. *Id.* at 68-69. Contrary to speculation by LabMD's expert, Mr. Fisk, that LabMD's router could provide significant additional network-level firewall protection, the record shows that, as configured, LabMD's router contributed little to data security. *See, e.g.*, CX0735 (Kaloustian IH) at 96-99; CX0678 at 10; CX0729. The Windows operating system used on the servers also had firewalls available, but LabMD often turned them off. CX0735 (Kaloustian IH) at 293-94.

[34] CX0719 (Hyer dep.) at 167-69. *See also* CX0731 (Truett dep.) at 68-69; CX0717 (Howard dep.) at 98-99; CX0735 (Kaloustian IH) at 115-16. Indeed, the firewall logs were erased by overwriting as frequently as every few days. CX0731 (Truett dep.) at 68-69; CX0710-A (Daugherty, LabMD Designee, dep.) at 176-77.

[35] Ans. ¶ 18(a); CX0755 at 4; CX0447 at 5-6; CX0730 (Simmons dep.) at 54-56; CX0735 (Kaloustian IH) at 269-70; CX0711 (Dooley dep.) at 117-19; CX0443 (LabMD Access Letter Response) at 13.

monitoring or a more complete walk-around inspection could have detected the program, but these safeguards were not in place.[36] Indeed, even after learning of the 1718 file breach in 2008, following which LabMD initiated daily "walk-around inspections," IT employees did not follow any written checklist and instead only asked employees if they were experiencing computer problems.[37]

B. LabMD Failed to Provide Data Security Training to its Employees

Even where basic hardware and software data security mechanisms are in place, there is an increased likelihood of exposing consumers' personal information if employees are not adequately trained. HIPAA's Security Rule, for example, requires that covered entities "[i]mplement a security awareness and training program for all members of [the] workforce (including management)."[38]

LabMD recognized the need for training, as acknowledged in its Compliance Manual which mandated that its compliance officer establish in-house training sessions regarding privacy and security,[39] but it failed to provide such training to any of its employees including its IT personnel.[40] As a result, employees, including sales representatives and billing staff, did not receive training regarding data security, security mechanisms, or the consequences of reconfiguring security settings in applications.[41] For example, the LabMD billing manager from May 2005 to May 2006 testified that she and other billing department employees did not receive any training from LabMD about protecting sensitive health data, stating that LabMD relied on the training that these employees received in their previous employment.[42] Due in part to this lack of data security training, LabMD employees appear not to have understood the risk involved in using P2P file sharing software on LabMD's computers.

C. LabMD Failed to Adequately Restrict and Monitor the Computer Practices of Individuals Using Its Network

LabMD also did not adequately limit or monitor employees' access to the sensitive personal information of patients or restrict employee downloads to safeguard the network.

[36] CX0735 (Kaloustian IH) at 92-93; CX0734 (Simmons IH) at 68-69; CX0705-A (Bradley dep.) at 46-47; Hill, Tr. 199-201; CX0740 (Hill Expert Report) ¶ 105; CX0707 (Bureau dep.) at 95-96. *See also* CX0719 (Hyer dep.) at 167-69 (If LabMD had monitored outgoing traffic for items like social security numbers, it could have detected the disclosure of the 1718 file.).
[37] CX0445 at 1-2; CX0730 (Simmons dep.) at 143; CX0719 (Hyer dep.) at 98-99.
[38] 45 C.F.R. §164.308(a)(5)(i). Other IT industry guidance provides: "Organizations should establish education and training programs to ensure that all users of information systems receive some minimum level of training in relevant security practices and knowledge regarding existing confidentiality policies. All computer users should complete such training *before* being granted access to any information systems." NRC Report at 174.
[39] CX0005 (LabMD Compliance Program, effective 2003) at 9.
[40] *See, e.g.*, CX0717 (Howard dep.) at 23-26; CX0711 (Dooley dep.) at 148-49; CX0707 (Bureau dep.) at 37-38, 105-06; CX0719 (Hyer dep.) at 130, 159-62: CX0735 (Kaloustian IH) at 208-20; CX0734 (Simmons IH) at 60-67.
[41] *See, e.g.*, CX0706 (Brown dep.) at 90-94; CX0711 (Dooley dep.) at 147-49; CX0714-A ([Former LabMD Employee] dep.) at 85-88; CX0734 (Simmons IH) at 61-62; CX0735 (Kaloustian IH) at 214-15; CX0708 (Carmichael dep.) at 25-26, 42.
[42] CX0706 (Brown dep.) at 96-98.

As the National Research Council has been emphasizing since 1997, "[p]rocedures should be in place that restrict users' access to only that information for which they have a legitimate need." NRC Report at 170. Similarly, HIPAA requires that covered entities implement policies and procedures for authorizing "access to electronic protected information" and "to prevent those workforce members who do not have access . . . from obtaining access to electronic protected health information." 45 C.F.R. § 164.308(a)(3)(i). LabMD's own 2004 employee handbook acknowledged that sharing health information unnecessarily was illegal and that the company was required to take "specific measures to ensure our compliance with this law."[43]

Yet, LabMD failed to employ adequate measures to prevent employees from accessing personal information not needed to perform their jobs. In fact, LabMD turned off the feature of its laboratory information software, LabSoft, that allowed for distinct access settings for different users. CX0717 (Howard dep.) at 117. Even college students hired on a part-time basis could access patients' medical and other sensitive information. CX0706 (Brown dep.) at 98-102. In addition, LabMD's sales representatives were able to use physician-clients' login credentials to log in to LabSoft, which gave them access to patient information. CX0718 (Hudson dep.) at 73-74, 88-89, 183. Because LabMD had no data deletion policy and never destroyed any patient or billing information it received since it began operating,[44] the amount of information on its network was extensive and included copies of personal checks and credit and debit card account numbers in addition to medical information.[45]

Nor did LabMD adequately restrict or monitor what employees downloaded onto their work computers. Throughout the period at issue, it was widely recognized that downloading unauthorized applications to a computer was dangerous, and P2P programs in particular "presented a well-known and significant risk that files would be inadvertently shared."[46] As the NRC also advised, "Organizations should exercise and enforce discipline over user software. At a minimum, they should . . . limit the ability of users to download or install their own software."[47]

Until at least the fall of 2009, LabMD's management employees were given administrative rights over their workstations and its sales employees had administrative rights

[43] CX0001 (LabMD Employee Handbook Rev. June 2004) at 6.
[44] CX0710-A (Daugherty, LabMD Designee, dep.) at 215; CX0733 (Boyle, LabMD Designee, IH) at 39-40; CX0443 at 6; CX0717 (Howard dep.) at 113.
[45] CX0716 (Harris dep.) at 19-25; CX0733 (Boyle IH) at 46.
[46] CX0738 (Shields Rebuttal Report)¶ 49; *see also id*. ¶¶ 40-48; CX0874 (SANS Institute InfoSec Reading Room Peer-to-Peer File-Sharing Networks Security) (2002) at 6; CX0878 (US-CERT - Risks of File-Sharing Technology) (2005) at 1 ("By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data . . . . The availability of this information may increase your risk of identity theft . . . .").
[47] NRC Report at 173; *see also* FTC Staff Report, *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues* (June 2005), *available at* https://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (noting the risk of inadvertent file-sharing on P2P platforms and methods for protecting against this risk).

over their laptop computers,[48] which allowed them to change security settings and download software applications and music files from the Internet.[49] LabMD's Policy Manual included a Software Monitoring Policy that stated that users' "'add/remove' programs file will be reviewed for the appropriate applications for the specific user."[50] If followed, this policy would have led to detection of the LimeWire program. CX0740 (Hill Report) ¶ 61(b).

In sum, if LabMD had followed proper data security protocols, LimeWire never would have been installed on the computer used by LabMD's billing manager in the first instance, or it would have been discovered and removed soon after downloading. Instead, LimeWire sat on the billing manager's computer for approximately three years and resulted in the exposure of the 1718 file.[51]

III. LabMD's Data Security Practices Were Unfair in Violation of Section 5(n)

We now turn to whether LabMD's data security practices were unfair within the meaning of Section 5(n). As discussed above, we find that LabMD's lax security practices resulted in the unauthorized sharing of the 1718 file on LimeWire, exposing sensitive medical information of 9,300 consumers to millions of Gnutella users. For the reasons discussed below, we further find that, due to the exposure of the 1718 file, LabMD's data security practices caused and were likely to cause substantial injury that was not avoidable by consumers or outweighed by countervailing benefits and thus that LabMD's data security practices were unfair.

We note that Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument.

[48] *See, e.g.*, CX0735 (Kaloustian IH) at 187-89; CX0705-A (Bradley dep.) at 147-49; CX0722 (Knox dep.) at 54-56; CX0719 (Hyer dep.) at 27- 31. In fact, at least until some point in 2005, all LabMD employees used the administrator's user name and password for their credentials. Consequently, all LabMD employees had the ability to exercise administrative rights for their computers, although not all LabMD computers had Internet access. CX0717 (Howard dep.) at 19-20; CX0735 (Kaloustian IH) at 166-72.

[49] CX0714-A ([Former LabMD Employee] dep.) at 38-40; CX0717 (Howard dep.) at 77; CX0735 (Kaloustian IH) at 167; CX0705-A (Bradley dep.) at 148-49.

[50] CX0006 (LabMD Policy Manual) at 18. In addition, LabMD's Employee Handbook stated "Personal internet or e-mail usage in the office is prohibited. . . . Computers in the office are property of LabMD and should only be used for company related reasons." CX0001 (LabMD Employee Handbook Rev. June 2004) at 7.

[51] *See supra* nn.4, 13.

A. LabMD's Data Security Practices Caused and Were Likely to Cause Substantial Injury

1. LabMD's Unauthorized Disclosure of the 1718 File Itself Caused Substantial Injury

We address first whether the unauthorized disclosure of the 1718 file caused actual "substantial injury" to consumers. The ALJ held that "privacy harms, allegedly arising from an unauthorized exposure of sensitive medical information . . . unaccompanied by any tangible injury such as monetary harm or health and safety risks, [do] not constitute 'substantial injury' within the meaning of Section 5(n)." ID 85 n.43. We disagree.

It is undisputed that the 1718 file contained names, dates of birth, social security numbers, insurance company names, policy numbers, and codes for laboratory tests performed, including tests for HIV, herpes, prostate cancer, and testosterone levels. IDF 82. We also know that the file was downloaded by at least one unauthorized third-party – Tiversa – and then shared with an academic researcher.

Complaint Counsel introduced evidence of a range of harms that can and often do result from the unauthorized disclosure of sensitive personal information of the types contained in the 1718 file. One category encompasses economic harms resulting from identity theft and medical identity theft. This includes monetary losses due to financial fraud and time and resources expended by consumers in resolving fraud-related disputes.[52] Medical identity theft associated with data breaches can also result in misdiagnosis or mistreatment of illness, and can thereby harm consumers' physical health and safety.[53] There is no dispute that these economic and health and safety harms fall squarely within the types of injury encompassed by Section 5(n).

Because LabMD never notified any of the consumers identified in the 1718 file that their information had been disclosed, we do not know whether the breach of the 1718 file resulted in actual identity theft, medical identity theft, or physical harm for any of the consumers whose information was disclosed. *See* Daugherty, Tr. 1087; CX0710-A (Daugherty dep.) at 48, 50. We therefore evaluate whether the disclosure of sensitive medical information alone, in the absence of proven economic or physical harm, satisfies the "substantial injury" requirement.

We conclude that the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n). For instance, Complaint Counsel's expert, Rick Kam, testified that disclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm."[54] Mr. Daugherty himself recognized the sensitivity of personal medical data and the gravity of its unauthorized disclosure.[55] In fact, the protection of personal

[52] *See* nn.71-72 and accompanying text, *infra*.
[53] ID 49-50; CX0742 (Kam Expert Report) at 15.
[54] CX0742 (Kam Expert Report) at 21; *see also id*. at 16; Kam, Tr. 411-12.
[55] *See* Daugherty, Tr. 989; CX0710-A (Daugherty Designee dep.) at 45.

health information was seen as part of the service LabMD delivered to its customers, and the company trained its sales representatives to assure physician clients that their data would be maintained on secure servers (despite not following through with such protections).[56] As LabMD's Vice President for Operations noted, it is vital for a lab to protect sensitive patient information.[57]

Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers. The Commission brought its very first data security case against Eli Lilly to address lax security practices that resulted in the inadvertent disclosure of the email addresses of Prozac users.[58] *FTC v. Eli Lilly & Co.*, 133 F.T.C. 763, 767-68 (2002) (complaint and consent order). A more recent example involving sensitive medical information is *GMR Transcription Services*. There we alleged that the failure of GMR's service provider to implement reasonable security measures harmed consumers due to the disclosure of files containing notes from medical examinations on the Internet, which included information about psychiatric disorders, alcohol and drug abuse, and pregnancy loss. *GMR Transcription Services, Inc.*, 2014 WL 4252393, *4 (Aug. 14, 2014) (complaint and consent order).[59] And just last month we announced a settlement with Practice Fusion, a cloud-based electronic health record company, for soliciting consumer healthcare reviews in a manner that we alleged failed to adequately disclose that the reviews would be posted on the Internet. We alleged that these practices resulted in the unauthorized disclosure of some patients' sensitive personal and medical information, including health conditions, medications taken, medical procedures performed, and treatments received. Complaint, *In re Practice Fusion, Inc.*, FTC File No. 142-3039 (June 8, 2015).[60]

There is also broad recognition in federal and state law of the inherent harm in the disclosure of sensitive health and medical information. Section 5(n) expressly authorizes us to look to "established public policies" as additional evidence in support of a determination about whether a practice is unfair, including whether it causes substantial injury, and we do so here.[61] Federal statutes such as HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as well as state laws, establish the importance of maintaining the privacy of medical information in particular. *See, e.g.*, HIPAA, 42 U.S.C. §§ 1320 et seq. (directing HHS to promulgate privacy and security rules for health information); 45 C.F.R. Parts 160 & 164 (privacy, data security, and related rules); HITECH Act, Pub. L. No. 111-5, 123 Stat. 226 (2009), *codified at* 42 U.S.C. §§ 300jj *et seq.*; §§ 17901 *et seq.*, and revisions to 42 U.S.C.

[56] CX0704-A (Boyle dep.) at 128-29; CX0718 (Hudson dep.) at 67-68.
[57] CX0704-A (Boyle dep.) at 128-29.
[58] This was brought as a deception case, but still demonstrates the Commission's concern with protecting sensitive medical information.
[59] *Available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.
[60] *Available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3039/practice-fusion-inc-matter.
[61] In highlighting the public policies about sensitive health and medical information established in these laws, we are not saying that practices are unfair simply because they offend those policies. Rather, such laws support our conclusion that the unauthorized exposure of sensitive health and medical information causes substantial consumer injury. *See* 15 U.S.C. § 45(n) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence;" however, public policy considerations may not "serve as a primary basis for [an unfairness] determination").

§§ 1320d—1320d(8); Freedom of Information Act, 5 U.S.C. § 552(b)(6) (restricting agencies from disclosing "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); Fair Credit Reporting Act, 15 U.S.C. §§ 1681a(i) & 1681b(g)(1) (generally prohibiting reporting agencies from releasing "a consumer report that contains medical information . . . about a consumer" for employment, credit, or insurance purposes)); *id*. § 1681a(i) (defining "medical information"); Ga. Code Ann. § 31-33-2(d) (forbidding release of medical records without patient's signed written authorization); *id.* § 31-22-4(c) (restricting clinical labs' disclosure of test results); *id.* §§ 31-22-9.1(a)(2)(D), 24-12-21(b)(1) (limiting the release of "AIDS confidential information," including the fact that a person has submitted to an HIV test); *id.* § 24-12-21(o), (u) (imposing criminal liability for intentional or knowing disclosure of AIDS confidential information and permitting civil liability for "gross negligence").

Federal courts have similarly acknowledged the importance of protecting the confidentiality of sensitive medical information. *See, e.g.*, *Maracich v. Spears*, 133 S. Ct. 2191, 2202 (2013) (recognizing that an individual's "medical and disability history" is among "the most sensitive kind of information" and characterizing its use in attorney solicitations as a "substantial . . . intrusion on privacy"); *Harris v. Thigpen*, 941 F.2d 1495, 1513-14 (11th Cir. 1991) (expressing view that prison inmates' interest in preventing non-consensual disclosure of their HIV-positive diagnoses, although not absolute, is "significant" and "constitutionally-protected"). State courts, including those in Georgia, also have long recognized a right to privacy in sensitive medical information. *See, e.g.*, *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E. 2d 491 (Ga. App. 1994) (en banc) (affirming verdict awarding damages for public disclosure of AIDS diagnosis).

Tort law also recognizes privacy harms that are neither economic nor physical. As explained by the Restatement of Torts, when "intimate details of [one's] life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy, unless the matter is one of legitimate public interest." RESTATEMENT (SECOND) OF TORTS § 652D, Comment b (1977). Thus, one can be held liable for invasion of privacy if "the matter publicized is of a kind that[:] (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* § 652D (summarizing tort of "publicity given to private life").[62]

We therefore conclude that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n), and thus that LabMD's disclosure of the 1718 file itself caused substantial injury.

[62] According to a Comment to this section, "if [a] record is one not open to public inspection, as in the case of income tax returns, it is not public, and there is an invasion of privacy when it is made so." *Id.* at Comment b. The D.C. Circuit has also affirmed the FTC's determination that certain debt-collection techniques are "unfair acts and practices" because they "invade the consumer's right of privacy, causing embarrassment and humiliation," and often harm consumers' reputations for financial stability and degrade their relationships with employers. *Credit Practices SBP*, 49 Fed. Reg. at 7744; *see Am. Fin. Servs. Ass'n*, 767 F.2d at 975 (affirming FTC's adoption of rule and finding such intangible consumer injuries were "neither trivial[,] speculative nor based merely on notions of subjective distress or offenses to taste").

2. LabMD's Unauthorized Exposure of the 1718 File Was Likely to Cause Substantial Injury

We now address whether, independent of our holding that the disclosure of sensitive medical information caused substantial injury under Section 5(n), the unauthorized exposure of the 1718 file for more than 11 months on LimeWire was also "likely to cause substantial injury." The ALJ interpreted "likely to cause" as requiring a showing that substantial consumer injury was "probable." ID 54, 90. He relied principally on the Merriam Webster dictionary's statement that "the word 'likely' is 'used to indicate the chance that something will happen,' and is primarily defined as 'having a high probability of occurring or being true.'" ID 54. On that basis, he concluded that Section 5(n) requires a showing that it is "probable that something will occur," not merely "possible," and that "at best, Complaint Counsel has proven the 'possibility' of harm."[63] ID 14, 54. The ALJ's analysis does not withstand scrutiny.

As an initial matter, we are unpersuaded by the ALJ's reliance on a single dictionary definition to determine the meaning of the phrase "likely to cause" in Section 5(n). Different dictionaries define the phrase differently. *See, e.g.*, Dictionary.com (defining "likely" as "reasonably to be believed or expected"). Some dictionaries define "likely" more broadly when used, as in Section 5(n), with an infinitive ("likely to cause"). Thus, Black's Law Dictionary defines "likely" in the phrase "likely to show" as "[s]howing a strong tendency; reasonably expected." *Black's Law Dictionary* (10th ed. 2014). Similarly, Collins English Dictionary defines "likely" when used as an adjective as "probable," but when used with an infinitive as "tending to or inclined."[64] None of these dictionary definitions is dispositive. Where there is disagreement about the meaning of an important statutory term, dictionary definitions may not be particularly helpful. *Bullock v. BankChampaign, N.A.*, 133 S. Ct. 1754, 1758 (2014). "It is a fundamental principle of statutory construction (and, indeed, of language itself) that the meaning of a word cannot be determined in isolation, but must be drawn" from the "specific context in which that language is used, and the broader context of the statute as a whole." *Yates v. United States*, 135 S. Ct. 1074, 1082 (internal quotations omitted).

[63] LabMD argues for an even higher threshold to assess likely causation, based on law used to determine whether a plaintiff has suffered an "injury in fact" for purposes of Article III standing. The standing doctrine "developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood" by "limit[ing] the category of litigants empowered to maintain a lawsuit in federal court" and, thereby, "prevent[ing] the judicial process from being used to usurp the powers of the political branches." *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016). Standing doctrine has no application here, where the issue is the authority of an executive branch agency to enforce the law, rather than the authority of federal courts to entertain a private party's lawsuit. Similarly, LabMD is wrong when asserting that the Commission must satisfy standing requirements before imposing a cease and desist order. The Commission, as an independent agency within the executive branch, is simply carrying out its duty to "take Care that the Laws be faithfully executed." U.S. Const. art. II, § 3. Indeed, the "injury in fact" prerequisite for standing is particularly inappropriate given Congress' empowerment of the FTC to "tak[e] preemptive action," consistent with "Section 5's prophylactic purpose." *FTC v. Freecom Communications, Inc.*, 401 F.3d 1192, 1203 (10th Cir. 2005).

[64] *See Collins English Dictionary Online, available at* http://www.collinsdictionary.com/dictionary/english/likely.

Unlike the ALJ, we agree with Complaint Counsel that showing a "significant risk" of injury satisfies the "likely to cause" standard.[65] In arriving at his interpretation of Section 5(n), the ALJ found that Congress had implicitly "considered, but rejected," text in the *Unfairness Statement* stating that an injury "may be sufficiently substantial" if it "raises a significant risk of concrete harm." ID 54-55 (citing *Unfairness Statement*, 104 F.T.C. at 1073 n.12). Yet the legislative history of Section 5(n) contains no evidence that Congress intended to disavow or reject this statement in the *Unfairness Statement*. Rather, it makes clear that in enacting Section 5(n) Congress specifically approved of the substantial injury discussion in the *Unfairness Statement* and existing case law applying the Commission's unfairness authority. *See* SENATE REPORT at 12-13; H.R. REP. NO. 103-617, at 12 (1994) (Conf. Rep.).

We conclude that the more reasonable interpretation of Section 5(n) is that Congress intended to incorporate the concept of risk when it authorized the Commission to pursue practices "likely to cause substantial injury." This reading is supported by prior Commission cases applying the unfairness standard, which also teach that the likelihood that harm will occur must be evaluated together with the severity or magnitude of the harm involved. In other words, contrary to the ALJ's holding that "likely to cause" necessarily means that the injury was "probable," a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low. For example, in *International Harvester* – the quintessential unfairness case – the Commission found the failure to include a warning label on a tractor gas cap to be unfair where harmful fuel geysering accidents had occurred at a "rate of less than .001 percent," but the injuries involved included death and severe disfigurement. *Int'l Harvester Co.*, 104 F.T.C. at 1063; *see also Philip Morris*, 82 F.T.C. at 16 (finding unfairness based on severe health hazards without alleging any injuries had yet occurred).

The Third Circuit interpreted Section 5(n) in a similar way in *Wyndham*. It explained that defendants may be liable for practices that are likely to cause substantial injury if the harm was "foreseeable," *Wyndham*, 799 F.3d at 246, focusing on both the "probability and expected size" of consumer harm. *Id*. at 255. This approach is consistent with the standard applied in negligence cases. As described in the Restatement of Torts, a "negligent act or omission may be one which involves an unreasonable risk of harm to another through . . . the foreseeable action of . . . a third person." RESTATEMENT (SECOND) OF TORTS § 302 (1965).

In this case, there was a significant risk of substantial injury. First, there was a high likelihood of harm because the sensitive personal information contained in the 1718 file was exposed to millions of online P2P users, many of whom could have easily found the file. The ALJ's contrary determination that the 1718 file could only have been found by a search of the file's exact name, IDF 77, was in error. Complaint Counsel's expert on the Gnutella network, Dr. Clay Shields, convincingly explained how the 1718 file could have been found through a variety of commonly-used search techniques that would not have required searching for its exact file name or components thereof.

[65] Complaint Counsel also argues that an act or practice that creates a "significant risk of concrete harm" thereby *causes* a substantial injury. We believe the practices in this case creating a significant risk of injury are more properly analyzed under the "likely to cause" portion of Section 5(n).

For instance, Dr. Shields pointed out that malicious users can and do search for P2P users whose computers are misconfigured. CX0738 (Shields Rebuttal Report) at ¶¶ 65-66. As he explained, a computer may be misconfigured to share files that the user does not intend to share, such as all the files in the "My Documents" directory. Shields, Tr. 868. Users do not need to have any information about the names of the files they hope to find; rather, they can look for common files that are placed in particular directories when installed (*e.g.*, in "My Documents"). CX0738 (Shields Rebuttal Report) at ¶ 65. Finding such files suggests a high probability that the computer is misconfigured and is exposing files that the user does not intend to share. *Id.* at ¶ 66. The searcher who locates such a computer can then use LimeWire's "browse host" function – which permits the searcher to see all the files the host computer is sharing, *id*. at ¶¶ 56-57 – to identify and download potentially sensitive files being inadvertently shared. *Id*. at ¶ 66; Shields, Tr. 844-45. "The LabMD computer, which was running LimeWire, would have been vulnerable to being found in this manner." CX0738 (Shields Rebuttal Report) at ¶ 67.

Dr. Shields explained further that these methods, including use of the browse host functionality, were not speculative – that P2P networks are often used by malicious persons who use these types of simple techniques to seek out information that has been inadvertently shared. *Id*. at ¶ 65. A user could have received a search hit for some other file that was present on the billing manager's computer and then used the browse host function to examine and download other files. Dr. Shields explained that because LabMD's billing manager was using LimeWire to download and share popular music that could result in many search hits, her behavior "could easily have led to the 1,718 File being downloaded through browse host." *Id*. at ¶ 57. He continued:

> In addition, the shared folders on [the billing manager's] computer contained other files that might have drawn the interest of potential thieves and could have been found through the basic search. For example, there was a file named "W-9 Form" being shared. A person who was interested in identity theft might have been searching [for] that term to find addresses and Social Security numbers. The browse host function could then be used to view and download the 1,718 File that was contained in the same shared folders.

Id. at ¶ 58.

Dr. Shields' conclusions are borne out by what actually occurred. Mr. Wallace did not discover the 1718 file by searching for its exact name. Rather, he located the 1718 file while conducting a general search for sensitive information on P2P networks, using standard P2P software. Wallace, Tr. 1342-43, 1372, 1440-41; IDF 122. There is nothing in Mr. Wallace's testimony to suggest that he was searching for LabMD files specifically or that he knew – or even could have known – the 1718 file's exact name.

Dr. Shields also opined that "[w]hile it may be unlikely that any random user would choose to download the 1,718 File, this low probability must be balanced against the enormous number of users on the Gnutella system." CX0738 (Shields Rebuttal Report) at ¶ 59. In particular, he quotes the estimate of LabMD's expert, Adam Fisk, that "[a]t any one time on the LimeWire network there would be approximately 2 to 5 million users online," and opines that

"[o]ver an extended period of time, such as weeks or months, even a 1 in 1,000,000 chance of someone downloading the 1,718 file would therefore result in it being downloaded many times." *Id.* at ¶¶ 60-61. Dr. Shields' opinion, in combination with Mr. Wallace's actual experience, is persuasive evidence that LabMD's exposure of the 1718 file and other documents[66] for sharing on the Gnutella network created a significant likelihood that sensitive medical and other information would be disclosed.[67] Indeed, the sensitivity of the data in LabMD's possession made a breach particularly likely to occur. As Complaint Counsel's expert Mr. Van Dyke noted, the types of sensitive personal information found on the 1718 file are very attractive to identity thieves. CX0741 (Van Dyke Expert Report) at 5-6, 12-13.

The ALJ nonetheless discounted Complaint Counsel's evidence that LabMD's practices were "likely to cause" harm in light of what he characterized as the "inherently speculative nature of predicting 'likely' harm." ID 53. He placed great weight on the fact that Complaint Counsel had "not . . . identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security" and concluded that this "undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless 'likely' to occur." ID 52; *see also id.* at 14, 64, 88.

The ALJ's reasoning comes perilously close to reading the term "likely" out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes. This is particularly true in the data security context. Consumers typically have no way of finding out that their personal information has been part of a data breach. CX0742 (Kam Expert Report) at 17; Kam, Tr. 400-02; *see also* ID 52. Furthermore, even if they do learn that their information has been exposed, it is very difficult for identity theft victims to find out which company was the source of the information that was used to harm them absent notification from the company. Kam, Tr. 398-99. Here, given the absence of notification by LabMD, a lack of evidence regarding particular consumer injury tells us little about whether LabMD's security practices caused or were likely to cause substantial consumer injury.[68] Moreover, Section 5 very clearly has a "prophylactic purpose" and authorizes the Commission to take "preemptive action." *FTC v. Freecom Commc'ns*, 401 F.3d 1192, 1203 (10th Cir. 2005).[69] We need not wait for consumers to suffer known harm at the hands of identity thieves.

[66] *See* IDF 127 ("Using the 'browse host' function, Mr. Wallace also downloaded 18 other LabMD documents in addition to the 1718 File, three of which contained Personal Information."). One of those documents contained names and passwords of LabMD employees; others contained the names and social security numbers or the names and insurance information for specific patients. *See* Wallace, Tr. 1405; RX645 at 39-43 (*in camera*).

[67] The ALJ found that LabMD had searched P2P networks for other users in possession of the 1718 file and found nothing. IDF 95-97. Neither the ALJ nor LabMD, however, have identified any evidence suggesting that a malicious user who downloaded the 1718 file would further share that file, rather than simply keep it for his or her own malicious use.

[68] Significantly, LabMD typically interacted only with physicians' offices and had no direct dealings with consumers, other than billing when insurance did not pay. Even consumers whose samples were tested by LabMD may not have known that the company was retaining their sensitive personal data. See CX0726 (Maxey dep.) at 78-81; CX0728 (Randolph dep.) at 67.

[69] *See also FTC v. Gratz*, 253 U.S. 421, 435 n.6 (1920) (Brandeis, J., dissenting) ("The purpose of this bill . . . is to seize the offender before his ravages have gone to the length necessary in order to bring him within the law that we

In addition to demonstrating a significant risk of harm in this case, Complaint Counsel also proved that the severity and magnitude of potential harm was high. As noted above, Complaint Counsel's expert witnesses identified a range of harms that can and do result from the unauthorized disclosure of consumers' sensitive personal information of the type maintained by LabMD on its computer network.

Mr. Kam focused on the consumer harms caused by medical identity theft, *i.e.*, the unauthorized use of a consumer's personal health information such as health insurance policy information, test codes, and diagnosis codes, to fraudulently obtain medical services, prescription drugs, or other products or services, or to fraudulently bill health insurance providers.[70] In particular, Mr. Kam reported the results of a Survey on Medical Identity Theft by the Ponemon Institute in 2013, showing the substantial out-of-pocket expenses that medical identity theft victims typically incur, including "reimbursement to healthcare providers for services received by the identity thief"; costs of "identity protection, credit counseling and legal counsel"; and "payment for medical services and prescriptions because of a lapse in healthcare coverage."[71] He observed that victims typically have to spend significant time to resolve problems caused by medical identity theft, and often give up because the process is so difficult and time-consuming. CX0742 at 15. He also noted that because "[t]here is no central 'medical identity bureau' where a consumer can set up a fraud alert, like they can with the credit bureaus," and as a result, "identity thieves can continue to use a consumer's medical identity to commit identity crimes" for long periods of time. *Id.* at 14.

Mr. Van Dyke emphasized that information like names, addresses, and Social Security numbers cannot be readily changed so that, once compromised, these types of personal information can often be used by malicious actors for an extended period and "could result in affected consumers suffering fraud in perpetuity." CX0741 at 5, 12. Mr. Van Dyke also cited data from a survey conducted by his firm, Javelin, showing the average amount of money that identity thieves steal, the average number of hours that victims spend to resolve specific categories of fraud, and the out-of-pocket costs that victims incur in the course of resolving them. *Id.* at 9-11.[72]

In addition, medical identity theft associated with data breaches can result in misdiagnosis or mistreatment of illness, and can thereby harm consumers' physical health and

already have.") (quoting 51 CONG. REC. 11455 (July 1, 1914) (statement of Sen. Albert Cummins, co-sponsor of the legislation ultimately enacted as the FTC Act)).

[70] CX0742 at 11-12. The risks of medical identity theft and its potentially serious consequences were well-known during the relevant time frame. *See, e.g.*, *Medical Identity Theft Environmental Scan, available at* https://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf (prepared by Booz, Allen, Hamilton for HHS and ONC for Health Information Technology, Oct. 2008); P. Dixon, *Medical Identity Theft: The Information Crime That Can Kill You, available at* https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/.

[71] CX0742 at 15. According to the Ponemon Survey and Mr. Kam, loss of insurance coverage as a result of medical identity theft is a serious problem. *Id*.

[72] Although Mr. Van Dyke bases his report primarily on the Javelin consumer survey conducted in 2013, Javelin has been conducting similar surveys for the past ten years.

safety. ID 49-50; CX0742 at 15. Mr. Kam explained that a "victim of medical identity theft may have the integrity of [his or her] electronic health record compromised if the health information of the identity thief has merged with that of the victim," and that "[t]he resulting inaccuracies may cause serious health and safety risks to the victim, such as the wrong blood type or life-threatening drug allergies." CX0742 at 15; Kam Tr. 426-27. Medical identity theft victims have also reported other types of health and safety harms caused by the theft, such as delay in receiving medical treatment and incorrect pharmaceutical prescriptions. CX0742 at 16. All of these types of harms are cognizable under Section 5(n).

Finally, given that we have found that the very disclosure of sensitive health or medical information to unauthorized individuals is itself a privacy harm, LabMD's sharing of the 1718 file on LimeWire for 11 months was also highly likely to cause substantial privacy harm to thousands of consumers, in addition to the harm actually caused by the known disclosure.[73]

Having found that the unauthorized exposure of the 1718 file created a high likelihood of a large harm to consumers, we conclude that the unauthorized exposure of the 1718 file was "likely to cause substantial injury to consumers."

3. The Sacramento Incident

We do not find, however, that the security incident involving the Sacramento documents provides additional evidence that LabMD's computer security practices caused or were likely to cause substantial injury. LabMD does not dispute that the Sacramento Police Department discovered the documents in the possession of identity thieves. However, unlike with the 1718 file incident, the evidence does not establish any causal link between the exposed documents, which were found in hard copy form, and LabMD's computer security practices.

The fact that the documents were found in the hands of identity thieves strongly suggests that they viewed the information contained therein (including names and social security numbers) as valuable for their purposes. It also raises concerns that LabMD's lax security practices may not have been confined to its computers. Nonetheless, like the ALJ, we conclude that Complaint Counsel have not established that the Sacramento security incident was caused by deficiencies in LabMD's *computer* security practices, which were the sole practices challenged in the Complaint. *See* Comp. ¶ 10.

B. Consumers Could Not Reasonably Avoid the Injuries Resulting from LabMD's Data Security Practices

Turning to the second prong of Section 5(n), we find that consumers had no ability to avoid the harms caused by LabMD's practices. LabMD's clients were physicians or other health care providers. Most patients who provided blood or tissue samples for testing were not notified that their specimens would be given to LabMD for testing, or that LabMD would receive and retain other sensitive personal information as well. CX0726 (Maxey, SUN Designee, dep.) at 78;

[73] *See* nn.54-62 and accompanying text, *supra*.

CX0728 (Randolph, Midtown Designee, dep.) at 67.[74] While some consumers eventually learned of LabMD's existence during the billing or collections process, even these consumers lacked any information about LabMD's data security practices, CX0726 (Maxey, SUN Designee, dep.) at 80-81, 100-01, and thus had no opportunity to avoid injuries caused by these practices. In sum, victims of a LabMD data breach would have "no chance whatsoever to avoid the injury before it occurred." *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008), *aff'd*, 604 F.3d 1150 (9th Cir. 2010).

LabMD nonetheless argues that consumers were reasonably capable of mitigating any injury "after the fact." We disagree. Our inquiry centers on whether consumers can avoid harm *before* it occurs.[75] Second, even assuming *arguendo* that the ability to mitigate harm does factor into its avoidability, there is nothing LabMD has pointed to that demonstrates mitigation after the fact would have been possible here. Without notice of a breach, consumers can do little to mitigate its harms. CX0742 (Kam Expert Report) at 17; Kam, Tr. 398-402. LabMD would be the entity to provide such notice if a breach occurred on its network, yet it did not notify the relevant 9,300 consumers that their medical and other sensitive personal information had been exposed in the 1718 file. CX0710-A (Daugherty Designee dep.) at 48; Daugherty, Tr. 1087. Moreover, even if consumers do receive notice that their information was involved in a breach, it may be difficult or impossible to mitigate or avoid further harm, since they have "little, if . . . any, control over who may access that information" in the future,[76] and tools such as credit monitoring and fraud alerts cannot foreclose the possibility of future identity theft over a long period of time.[77] Furthermore, consumers cannot avoid or fully reverse certain categories of non-economic injury that may accompany the exposure of sensitive medical information. In short, there was no way for consumers to avoid the injury that was caused or likely to be caused by LabMD's inadequate data security practices.

C. The Injuries Were Not Outweighed by Countervailing Benefits to Consumers or to Competition

Finally, we must consider whether the consumer injury resulting from LabMD's data security practices is "outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). A "benefit" can be in the form of lower costs and then potentially lower prices for consumers, and the Commission "will not find that a practice unfairly injures consumers unless it is injurious in its net effects." *Unfairness Statement*, 104 F.T.C. at 1073. This cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk

[74] Moreover, LabMD also holds personal data of approximately 100,000 consumers for whom it never performed tests. JX0001-A (Joint Stipulations) at 3; CX0710-A (Daugherty dep.) at 185-90, 192-93, 198.

[75] *See, e.g., In re Orkin Exterminating Co.*, 108 F.T.C. at 366 (holding that "[a]nticipatory avoidance through consumer choice was impossible" when consumers had no "reason to anticipate the impending harm" and respondent did not give most consumers information on "the means to avoid it") (quoted with approval in *Orkin*, 849 F.2d at 1365).

[76] For example, in the case of an unauthorized release of information through a P2P network, "once a file has been shared on a P2P network it can be difficult or impossible to remove it from the network." CX0738 (Shields Rebuttal Report) ¶ 21.

[77] Kam, Tr. at 402; CX0742 (Kam Expert Report) at 22-23.

of such injury. *Int'l Harvester Co.*, 104 F.T.C. at 1064. When a case concerns the failure to provide adequate data security in particular, "countervailing benefits" are the foregone costs of "investment in stronger cybersecurity" by comparison with the cost of the firm's existing "level of cybersecurity." *Wyndham*, 799 F.3d at 255.

Here, we conclude that whatever savings LabMD reaped by forgoing the expenses needed to remedy its conduct do not outweigh the "substantial injury to consumers" caused or likely to be caused by its poor security practices. For the data security failures we described above, the record contains detailed evidence of low-cost solutions that LabMD could have adopted to cure the deficiencies and render its practices reasonable and appropriate. LabMD has not disputed Complaint Counsel's showing as to the availability and cost of these alternatives.

For example, there were many free or low cost software tools and hardware devices available for detecting vulnerabilities, including antivirus programs, firewalls, vulnerability scanning tools, intrusion detection devices, penetration testing programs,[78] and file integrity monitoring tools.[79] CX0740 (Hill Expert Report) ¶ 65. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost. Hill, Tr. 194; CX0740 (Hill Expert Report) ¶ 101. Remediation processes and updates for vulnerabilities were widely available. CX0740 (Hill Expert Report) ¶ 99. These processes included free notifications from vendors, as well as the Computer Emergency Response Team ("CERT"), the Open Source Vulnerability Data Base, NIST, and others. *Id.*

In addition, LabMD could have adequately trained employees to safeguard personal information at relatively low cost. Hill, Tr. 173-76; CX0740 (Hill Expert Report) ¶ 92. Several nationally recognized organizations provided low-cost or free IT security training courses. Hill, Tr. 173-74; CX0740 (Hill Expert Report) ¶ 89 & n.30. For example, the SysAdmin Audit Network Security (SANS) Institute, formed in 1989, provides free security training webcasts. Additional free resources could be found online, and CERT at Carnegie Mellon University offered e- learning courses for IT professionals for as little as $850. Hill, Tr. 174-75; CX0740 (Hill Expert Report) ¶ 89 n.30.

LabMD also could have limited employees' access to only the types of personal information that they needed to perform their jobs at relatively low cost. Hill, Tr. 166-67; CX0740 (Hill Expert Report) ¶ 85. Because operating systems and applications already have access controls embedded in them, rectifying this issue would have required only the time of trained IT staff. Hill, Tr. 166-67; CX0740 (Hill Expert Report) ¶ 85. In addition, LabMD could have purged the personal information of consumers for whom it never performed testing at

[78] Since 1997, several well-respected and free penetration test and network analysis mechanisms have been available. Examples include Wireshark (released in 1998 under a different name), Nessus (free until 2008), and nmap (released in 1997). Hill, Tr. 162; CX0740 (Hill Expert Report) ¶ 71. When LabMD hired outside IT service provider ProviDyn to conduct penetration tests after the FTC investigation began, in May 2010, the cost for nine tests was $450. CX0044 at 4; CX0048; CX0488 at 4.

[79] LabMD could have implemented SNORT, a respected and widely used intrusion detection system, which has been available at no cost since 1998. CX0740 (Hill Expert Report) ¶¶ 69 n.22, 104(h). Free file integrity monitoring products, such as Stealth and OSSEC, were also available to LabMD during the relevant time period. CX0740 (Hill Expert Report) ¶ 69 n.22.

relatively low cost. This could have been accomplished using LabMD's database applications, and would have required only the time of trained IT staff. Hill, Tr. 164; CX0740 (Hill Expert Report) ¶ 80(b). We recognize that the time of trained IT staff can amount to a real cost, but LabMD already had multiple IT personnel on staff. Any such additional costs would be far outweighed by the likely adverse consequences to consumers of LabMD's lax security practices.

Finally, LabMD readily could have prevented the installation of LimeWire by simply providing the billing manager and other employees non-administrative accounts on their workstations. CX0740 (Hill Expert Report) ¶¶ 85, 104(a). The Windows operating system that LabMD used included this functionality; LabMD could have made use of it with no monetary expense. *Id.*

Consequently, the benefits resulting from LabMD's flawed practices are negligible because the costs to provide the appropriate data security would have been relatively low. The cost-benefit test "is easily satisfied 'when a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition.'" *Neovi*, 598 F. Supp. 2d at 1116 (quoting *FTC v. J.K. Publications, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000)). That is the case here.

IV. None of LabMD's Affirmative Defenses or Other Objections Has Merit

A. Fair Notice and Due Process

LabMD's First Amended Answer raised six affirmative defenses, most of which we have already addressed in prior rulings or elsewhere in this Opinion.[80] Our discussion here focuses on LabMD's fifth affirmative defense: that this proceeding violates its Fifth Amendment due process rights and the Administrative Procedure Act because the Commission failed to provide adequate notice of what data security practices are required by Section 5. Although we addressed essentially the same arguments and explained why they are meritless in our January 16, 2014 order, LabMD reiterates and expands on them in the present appeal.

First, LabMD contends that our unfairness standard is "void for vagueness," in violation of the Fifth Amendment. As we noted in our January 16, 2014 order, the Supreme Court and courts of appeals have rejected comparable due process challenges on many occasions and affirmed agency and lower court decisions imposing liability for violations of statutes that, like the FTC Act, use broad terms such as "unfair," "unjust," or "unreasonable" to define which practices are prohibited. *See* Comm'n Order Denying Motion to Dismiss at 15. For example,

[80] We rejected LabMD's first, second, and third affirmative defenses – respectively, the failure to state a claim upon which relief can be granted, absence of subject matter jurisdiction, and an absence of statutory authority to regulate the acts or practices alleged – in our January 16, 2014 order. We also rejected LabMD's contention that its acts and practices were not "in or affecting commerce," as defined in Section 4 of the FTC Act. Comm'n Order Denying Motion to Dismiss at 17. LabMD's fourth defense is that the acts or practices alleged in the Complaint do not constitute a violation of Section 5(n). That assertion is addressed throughout this Opinion, in which we analyze the evidence establishing that LabMD's data security practices satisfied each of the elements in Section 5(n). Finally, we rejected LabMD's sixth affirmative defense (challenging the ALJ's role as presiding officer) in our September 14, 2015 order.

courts and agencies often evaluate restraints of trade under Sections 1 and 2 of the Sherman Act, as well as under the FTC Act's prohibition of "unfair methods of competition," 15 U.S.C. §§ 1, 2, 45(a), using a fact-specific "rule of reason." *See, e.g., FTC v. Indiana Fed. of Dentists*, 476 U.S. 447, 457-59 (1986). For over a century, courts have held that this flexible "rule of reason" standard does not violate defendants' due process rights. *See, e.g., Standard Oil Co. v. United States*, 221 U.S. 1, 66-69 (1911). Similarly, courts have held that agencies may, "consistent[] with the obligations of due process," enforce the prohibitions of "unjust" or "unreasonable" rates or practices in various public utility and common carrier regulatory statutes. *See Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968); *see also FPC v. Hope Natural Gas Co.*, 320 U.S. 591, 601-02 (1944); *Verizon Commc'ns, Inc. v. FCC*, 535 U.S. 467, 477, 481 (2002).

LabMD's vagueness challenge relies heavily on *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012), in which the Federal Communications Commission imposed substantial monetary forfeitures on broadcasters for violating a statute that prohibited broadcast "indecency." But *Fox* is distinguishable from this case in a number of important respects. The regulatory action in *Fox*, penalizing broadcasters based on the content of the language in their programs, directly implicated their First Amendment right to free speech. 132 S. Ct. at 2317. No comparable fundamental right is at issue here. LabMD cannot plausibly contend that it had a constitutional right to manage its computer networks in a manner that was likely to expose sensitive personal information to unauthorized third parties. *See Wyndham*, 799 F.3d at 255 (lower level of statutory notice was required because "[S]ection 45(a) does not implicate any constitutional rights") (citing *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982)).

Moreover, in *Fox*, the agency applied a criminal statute, 18 U.S.C. § 1464, and imposed monetary penalties. By contrast, Section 5 of the FTC Act is a civil statute and only injunctive relief is at issue in this case, not criminal or "quasi-criminal" fines. *Wyndham*, 799 F.3d at 255 & n.20 (citing *Flipside*, 455 U.S. at 498-99, and *Ford Motor Co. v. Texas Dept. of Transp.*, 264 F.3d 493, 508 (5th Cir. 2001)). Section 5 therefore is "subject to a less strict vagueness test." *Flipside*, 455 U.S. at 498.

Additionally, in *Fox*, the agency abruptly reversed a more lenient interpretation to which it had adhered for decades, and imposed liability in a manner that "failed to provide . . . fair notice of what is prohibited." 132 S. Ct. at 2318 (internal quotations omitted). The Court has faulted other abrupt changes of policy for similar reasons in other cases. *See, e.g., Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 (2012) (invalidating agency's "interpretation of ambiguous regulations [that] impose[d] potentially massive liability on respondent for conduct that occurred well before that interpretation was announced" – which was "precisely the kind of 'unfair surprise' against which our cases have long warned"); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 146-47 (2000) (overturning rules in part because agency had repeatedly and consistently stated that it lacked authority to regulate tobacco products). By contrast, here the FTC is imposing the same basic data security standard it has consistently articulated for nearly fifteen years.

LabMD challenges this enforcement proceeding next on the ground that the Commission had "not prescribed regulations or legislative rules under Section 5 establishing medical data security standards" before issuing the complaint against LabMD. In our January 16, 2014 order, we noted that "longstanding case law confirm[s] that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue." Comm'n Order Denying Motion to Dismiss at 14 (citing *SEC v. Chenery*, 332 U.S. 194, 201-02 (1947), and *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974)). Indeed, "complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings." *Id.* at 14-15. By the same token, "it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified," and thus "courts and juries [routinely] subject companies to tort liability for violating uncodified standards of care." *Id.* at 16-17.

Fundamentally, Section 5(n) provides reasonably clear and intelligible guidelines for companies to follow in designing their own data security programs. *See Wyndham*, 799 F.3d at 255. As discussed above, the FTC Act simply requires a company that maintains personal information about consumers to assess the risks that its actions could cause harm to those consumers and to implement reasonable measures to prevent or minimize such foreseeable harm.

We provided ample notice to the public of our expectations regarding reasonable and appropriate data security practices by issuing numerous administrative decisions finding specific companies liable for unreasonable data security practices. Our complaints, as well as our decisions and orders accepting consent decrees, which are published on our website and in the Federal Register, make clear that the failure to take reasonable data security measures may constitute an unfair practice. Those complaints, decisions, and orders also flesh out the specific types of security lapses that may be deemed unreasonable.[81] These widely available materials

[81] *See, e.g.*, *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005); *CardSystems Solutions, Inc.*, 71 Fed. Reg. 10686 (FTC, Mar. 2, 2006) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch); *DSW Inc.*, 141 F.T.C. 117 (2006); *Reed Elsevier, Inc.*, (FTC, July 29, 2008) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter); *TJX Companies, Inc.*, (FTC, July 29, 2008) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter). The FTC has also provided substantial public guidance outside the litigation context. *See* CX0771 at 2 (Press Release: Press Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure (Apr. 2, 2004)) (recommending that businesses "prohibit[] [their] employees from installing file-sharing programs on their computers"); FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2007) (announced in FTC's press release "FTC Unveils Practical Suggestions for Businesses on Safeguarding Personal Information" (Mar. 8, 2007), *available at* https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding) (advising companies, *inter alia*, to "[k]eep sensitive data in your system only as long as you have a business reason to have it"; "[a]ssess the vulnerability of each connection to commonly known or reasonably foreseeable attacks"; "[s]can computers on your network to identify and profile the operating system and open-network services"; "[m]onitor outgoing traffic for signs of a data breach"; and "[t]ake time to explain the rules to your staff, and train them to spot security vulnerabilities"). *See also* 16 C.F.R. Part 314 (FTC standards for safeguarding consumers' financial information, promulgated pursuant to the Gramm-Leach-Bliley Act); 65 Fed. Reg. 54186 (Sept. 7, 2000) (advance notice of proposed rulemaking and request for comment on Part 314 rules); 66 Fed. Reg. 41162 (Aug. 8, 2001) (proposed rule); 67 Fed. Reg. 36484 (May 23, 2002) (final Part 314 rule and Statement of Basis and Purpose).

"constitute a body of experience and informed judgment to which . . . [parties] may properly resort for guidance." *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976). And even though they "are neither regulations nor 'adjudications on the merits,'" they are sufficient to afford fair notice of what was needed to satisfy Section 5(n). *See Wyndham*, 799 F.3d at 257 (citing *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004); *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008); and *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995)). LabMD cannot seriously contend that it lacked notice that its security failures, which led to at least one documented breach of thousands of consumers' sensitive personal information – practices similar to those committed by other companies against which the FTC has taken action – could trigger Section 5 liability.[82]

B. Exclusion of All Evidence as Claimed "Fruit of the Poisoned Tree"

We concur with the ALJ's conclusions that the testimony of Robert Boback, CEO of Tiversa, was not credible or reliable. IDF 160, 166-68; ID 60. In particular, we agree that Mr. Boback's assertion that Tiversa had gathered evidence showing that the 1718 file had spread to multiple Internet locations by means of LimeWire was false and that the document that purported to list Internet locations where the 1718 file had been found (CX0019) was unreliable. IDF 129, 148-49, 153-54; ID 60. Complaint Counsel do not take issue with these conclusions in their appeal. They represent that they have not relied on Mr. Boback's testimony or on CX0019 here or in their pre- or post-trial briefs before the ALJ.

LabMD nonetheless argues that all of the evidence obtained by Complaint Counsel should have been excluded from the record. According to LabMD, Complaint Counsel "knew, or should have known" that Tiversa was not authorized to obtain the 1718 file, that all of Complaint Counsel's evidence was the direct "fruit" of the 1718 file, and thus that the entire case should have been dismissed. RAB 64. This argument fails.

First, the record does not show that Tiversa, whatever its motives, unlawfully obtained the 1718 file; LabMD made the file freely available for public viewing through LimeWire. Moreover, even evidence improperly obtained by private individuals and provided to law enforcement officials is not excluded unless the private actors served as agents of the government. *See, e.g., United States v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990) ("[T]he exclusionary rule of the Fourth Amendment does not apply to a search and seizure by a private person not acting in collusion with law enforcement officials in order to circumvent the requirements of a search warrant.").

As the Court of Appeals for the Eleventh Circuit has explained, "the exclusionary rule is designed to deter police misconduct, rather than to punish the errors of others," so that "[m]isconduct by other actors is a proper target of the exclusionary rule only insofar as those

[82] *See, e.g., BJ's Wholesale Club*, 140 F.T.C. at 467, ¶ 7(4) (2005) (alleging that BJ's "failed to employ sufficient measures to detect unauthorized access or conduct security investigations"); *DSW, Inc.*, 141 F.T.C. at 119, ¶ 7(5) (2006) (alleging that DSW "failed to employ sufficient measures to detect unauthorized access"); Comp. ¶ 10(g) (alleging that LabMD "did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks").

others are adjuncts to the law enforcement team." *United States v. Herring*, 492 F.3d 1212, 1217 (11th Cir. 2007) (internal quotations omitted). Accordingly, the exclusionary rule applies only in "those areas where its remedial objectives [*i.e.*, deterring law enforcement agents from violating the Fourth Amendment] are thought most efficaciously served." *United States v. Calandra*, 414 U.S. 338, 348 (1974). Furthermore, the Supreme Court has made clear that the government does not violate due process by reason of improper private conduct so long as the agency did not "exercise[] coercive power or . . . provide[] such significant encouragement, either overt or covert," to induce the private actors to commit such purportedly unlawful conduct. *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982).

There is no evidence that Tiversa acted as an "agent" or "adjunct" to the FTC in obtaining the 1718 file, much less that anyone at the FTC "exercised coercive power" compelling Tiversa to do so. Consequently, even granting that Tiversa was financially motivated to obtain confidential information, there was nothing improper about Commission staff's receipt of the information via a civil investigative demand in a law enforcement matter.[83]

This case is thus entirely distinguishable from the principal case on which LabMD relies, *Knoll Associates, Inc. v. FTC.*, 397 F.2d 530 (7th Cir. 1968), in which the court concluded that Complaint Counsel's "use of . . . stolen documents render[ed] the Commission's order unenforceable." *Id*. at 533-34. In that case, undisputed evidence showed that a former sales representative had stolen the documents "for the purpose of assisting the Commission counsel in the prosecution of the proceeding," and that Complaint Counsel "knowingly gave its approval to [his] unlawful act." *Id.* at 533. None of those factors is present here. No proceeding against LabMD was pending when Tiversa obtained the 1718 file and nothing in the record indicates that Tiversa was acting at the direction or behest of FTC staff.[84]

[83] LabMD's assertion that the use of the Privacy Institute "as a PHI conduit made the government a party to conduct which violated HIPAA," RAB 64, is unclear. As described in the Initial Decision, the FTC issued its civil investigative demand to the Privacy Institute, a Tiversa affiliate created for the purpose of receiving the CID. IDF 136-38. LabMD does not explain why directing the CID to a Tiversa affiliate, rather than to Tiversa itself, made the FTC a party to a HIPAA violation. We see no factual or logical relationship between the manner in which the FTC staff obtained information from Tiversa and the manner in which Tiversa obtained the information in the first place.

[84] The ALJ found, based on Mr. Wallace's testimony, that after the meeting between Tiversa and FTC staff in the fall of 2009, Mr. Boback directed Mr. Wallace to generate false information purporting to show that the 1718 file had spread to multiple locations on the Internet and could be downloaded from those locations. IDF 146-49. LabMD apparently asks us to infer that FTC staff asked Tiversa to generate such false information in order to use it as evidence against LabMD. However, there is no basis whatsoever for such an inference. At trial, Mr. Wallace thoroughly discussed both his contacts with the FTC and Mr. Boback's directions regarding creation of evidence that the 1718 file had spread to multiple locations. At no time did he suggest that FTC staff knew of, or in any way acquiesced in, Mr. Boback's direction, much less that FTC staff had asked or suggested that such evidence be generated. *See* Wallace Tr. 1347, 1369-70, 1380, 1383-90, 1408-09, 1447. LabMD's related argument – that the FTC knew or should have known that Mr. Boback's testimony was untruthful, so that any continuation of this proceeding violates LabMD's due process rights – is similarly flawed. LabMD presents no factual basis for the assertion that Complaint Counsel knew or should have known that Mr. Boback's testimony was false, and no explanation why continuation of the proceeding *without* continued reliance on Mr. Boback's testimony violates due process.

C. Miscellaneous Objections and Defenses

Over the course of the proceeding, LabMD raised a number of objections to the procedures that the Commission used to conduct this administrative proceeding. None of these objections has merit. First, LabMD challenged the participation of Chief Administrative Law Judge D. Michael Chappell and Chairwoman Edith Ramirez. The Commission rejected both challenges.

Similarly, LabMD argued before the ALJ that the Commission as a whole has infringed LabMD's due process rights because the Commission purportedly has prejudged the outcome of the case. Specifically, LabMD claimed that it was denied due process because there was a "statistical certainty" that the Commission would "find LabMD's data security practices are unfair under Section 5(n) no matter what [the ALJ] does," and that "[t]his clear inevitability of outcome transforms the adjudicatory process into punishment." Resp't's Post-Trial Br. at 58. The argument is meritless. LabMD submitted no evidence that the Commission had "made up [its] mind about important and specific factual questions and [was] impervious to contrary evidence" before deciding this case. *Metro. Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1165 (D.C. Cir. 1995) (internal quotations omitted). Nor did LabMD show that the Commission had "in some measure adjudged the facts as well as the law of a particular case in advance of hearing it." *Cinderella Career & Finishing Sch., Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970) (internal quotations omitted). Rather, as is evidenced by this Opinion, we have decided the contested factual and legal issues on their merits, based on a careful analysis of the record. *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 493, 496-97 (1951); *see also FTC v. Cement Inst.*, 333 U.S. 683, 701-02 (1948) (rejecting claim that FTC's prior conclusions about legal issues denied respondent due process); *Kennecott Copper Corp. v. FTC*, 467 F.2d 67, 79 (10th Cir. 1972) (noting "the courts have uniformly held" that the fact that "the Federal Trade Commission combines the functions of investigator, prosecutor and judge and that Congress designed it in that manner . . . . does not make out an infringement of the due process clause of the Fifth Amendment").

Finally, we find that any defenses or arguments not raised on appeal by LabMD have been waived.[85] *See United States v. Jernigan*, 341 F.3d 1273, 1283 n.8 (11th Cir. 2003) ("a party seeking to raise a claim or issue on appeal must plainly and prominently so indicate"; otherwise, the issue "will be considered abandoned").

[85] In a single sentence in its post-trial brief before the ALJ, LabMD asserted that the FTC violated its First Amendment rights when it issued the Complaint in order "to retaliate against LabMD for speaking out against government overreach." Resp't's Post-Trial Br. 59. Apart from this one sentence, LabMD submitted no explanation of the basis for this argument. The single case LabMD cited in support of this contention, *Trudeau v. FTC*, 456 F.3d 178, 190-91 & n.22 (D.C. Cir. 2006), is inapposite. In that case, the D.C. Circuit affirmed the lower court's dismissal of a party's First Amendment claim against the FTC, but held that the court mistakenly dismissed the case for lack of subject-matter jurisdiction when it should have dismissed it for failure to state a claim. In any case, LabMD has cited no evidence in support of its argument. LabMD has therefore waived any possible First Amendment argument.

V. The Remedy is Appropriate and Required to Prevent Further Consumer Injury

Having found that LabMD violated the FTC Act, we enter an order that will ensure LabMD reasonably protects the security and confidentiality of the personal consumer information in its possession. 15 U.S.C. § 45(b); *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 428 (1957). "The Commission is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965) (internal quotations omitted). Rather, "[t]he Commission has wide latitude in fashioning orders to prevent . . . respondents from pursuing a course of conduct similar to that found to have been unfair." *Thompson Med. Co.*, 104 F.T.C. 648, 832-33 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986). This discretion is subject to two constraints, however. First, the order must be sufficiently clear and precise to be understood by the violator. *See, e.g.*, *Colgate-Palmolive*, 380 U.S. at 392. Second, the order must bear a reasonable relationship to the unlawful practice found to exist. *See, e.g.*, *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946).

We enter an order similar to the Notice Order that was attached to the Complaint. The Order contains three provisions to prevent future violations by LabMD and remediate the risk of harm to consumers.

Part I of the Order requires LabMD to establish, implement, and maintain a comprehensive information security program that is reasonably designed to protect the security and confidentiality of consumers' personal information. The program must be in writing, and should contain administrative, technical, and physical safeguards appropriate to LabMD's size and complexity, the nature and scope of its activities, and the sensitive personal information maintained on LabMD's network. In light of the discussion in our opinion and the availability of guidance about comprehensive information security programs from HIPAA and organizations such as NIST and the SANS Institute,[86] this provision is sufficiently clear and precise that its requirements can be readily understood and met.

Part II of the Order requires LabMD to obtain initial and then biennial assessments and reports regarding its implementation of the information security program. Each assessment must set forth the safeguards that LabMD implemented and maintained during the reporting period and certify that LabMD's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected. The assessments and reports must be provided by a qualified, objective, independent third-party professional. This provision will ensure that LabMD implements information security practices that are appropriate for LabMD's size, complexity, and the nature and scope of its activities and the sensitive personal information maintained on its network, and thereby complies with the Order. Courts have upheld the use of extensive assessment and monitoring requirements by an independent third party in final injunction orders. *See, e.g.*, *United States v. Apple, Inc.*, 992 F.Supp.2d 263 (S.D.N.Y. 2014), *aff'd*, 787 F.3d 131 (2d Cir. 2015).

[86] The FTC also offers guidance. *See, e.g.*, FTC, *Start with Security: A Guide for Business* (2015), *available at* www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

These two provisions are reasonably related to the unlawful practices that form the basis for LabMD's liability – the failure by LabMD to implement reasonable and appropriate data security practices to protect consumers' sensitive medical and other information – and seek to ensure that this failure is remedied. The FTC has required these types of provisions in numerous final orders to settle actions involving data security practices that it charged were violations of Section 5(n). *See, e.g., FTC v. Cornerstone & Co., LLC*, Case No. 1:14-cv-01479-RC, at 5-6, Sec. II (Stip. Final Order for Permanent Inj.) (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc; *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830-RC, at 4-6, Sec. II (Stip. Final Order for Permanent Inj.) (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc.

Part III of the Order requires LabMD to notify individuals whose personal information LabMD has reason to believe was or could have been exposed about the unauthorized disclosure of their personal information. LabMD must also notify the health insurance companies for these individuals of the information disclosure. Without notification, consumers would not know about the unauthorized disclosure of their sensitive information and would not know to take actions to reduce their risk of harm from identity or medical identity theft. LabMD acknowledges that this type of notice is required under HIPAA for disclosures of personal medical information that have occurred since 2010. Daugherty, Tr. 1020-21. Similarly, notice to affected consumers' insurance companies enables these insurers to protect consumers' identities from misuse. These notification requirements are consistent with relief obtained in other cases. *See FTC v. Cornerstone & Co., LLC*, Case No. 1:14-cv-01479-RC, at 7, Sec. IV (Stip. Prelim. Inj.) (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc; *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830-RC, at 7, Sec. IV (Stip. Prelim. Inj.) (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc.

The remaining parts of the Order are standard recordkeeping and sunset provisions that are included in most Commission orders. Part IV is a record-keeping requirement. Part V establishes that copies of the Order be distributed to, among others, principals, managers, and employees of LabMD. Part VI requires that LabMD file notifications about changes in corporate structure. Part VII establishes compliance reporting requirements. *See, e.g., FTC v. Direct Mktg. Concepts, Inc.*, 648 F. Supp. 2d 202, 213 (D. Mass. 2009) ("Courts have also included monitoring provisions in final orders in FTC cases to ensure compliance with permanent injunctions."); *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1018 (N.D. Ind. 2000) (ordering record retention, notification of changed employment or residence, access to premises, and monitoring); *FTC v. U.S. Sales Corp.*, 785 F. Supp. 737, 753 (N.D. Ill 1992) ("The order should also require Defendants to report their addresses and places of employment or business, and any subsequent changes in this information to the F.T.C."). Part VIII provides that the Order will terminate in 20 years. *See U.S. Sales Corp.*, 785 F. Supp. at 754 (explaining that a complex case "may require a sustained period of monitoring by the F.T.C. to ensure adequate compliance").

Complaint Counsel also seek a provision to require notice to the medical insurance companies for the consumers identified in the day sheets that were recovered in Sacramento.

(LabMD has already provided notice to the individuals whose information was disclosed in the Sacramento incident.) We do not include this provision from the Notice Order that was attached to the Complaint because such relief is not reasonably related to the violation in this case. LabMD's liability is not based on the Sacramento security incident, because we, like the ALJ, conclude that Complaint Counsel have not established that the Sacramento security incident was caused by deficiencies in LabMD's computer security practices. In addition, the day sheets included consumers' names, social security numbers, and copies of personal checks, but did not include medical or insurance information. IDF 182, 183, 185. The absence of medical or insurance information in this unauthorized disclosure provides further reason not to require notice to consumers' medical insurers.

LabMD contends that the relief in the Order is unnecessary and punitive. We disagree. Although LabMD stopped accepting specimen samples and conducting tests in January 2014, LabMD continues to exist as a corporation and has not ruled out a resumption of operations. IDF 36, 40-41; CX0709 (Daugherty dep.) at 15; Daugherty Tr., 1049-54. Moreover, LabMD continues to maintain the personal information of approximately 750,000 consumers on its computer system. IDF 42. Because LabMD continues to hold consumers' personal information and may resume operations at some future time, the Order is appropriate and necessary. *See, e.g.*, *Direct Mktg. Concepts, Inc.*, 648 F. Supp. 2d at 215 (imposing injunction "[e]ven though the . . . defendants currently have no employees and are not engaged in any business, they could resume such activities in the future"); *United States v. Bldg. Inspector of Am., Inc.*, 894 F. Supp. 507, 521 (D. Mass. 1995) (finding injunction appropriate where company had ceased operation but "remains a going concern and could resume at any time"); *cf. Int'l Harvester Co.*, 104 F.T.C. at 1067 ("[A]n obligation should ordinarily extend as long as the risk of harm exists.").

In addition, the Order takes account of LabMD's current limited operations. The Order requires that LabMD establish and implement a comprehensive information security program that provides administrative, technical and physical safeguards that are appropriate for the nature and scope of LabMD's activities. Order, ¶ 1. A reasonable and appropriate information security program for LabMD's current operations with a computer that is shut down and not connected to the Internet will undoubtedly differ from an appropriate comprehensive information security program if LabMD resumes more active operations.

Finally, we reject LabMD's claim that the Order is punitive. The Order merely requires measures reasonably necessary to ensure the protection of the personal information on its computer system and notice related to its unfair practices. An order that is purely remedial and preventative is not a penalty or forfeiture. *See Riordan v. SEC*, 627 F.3d 1230, 1234 (D.C. Cir. 2010).

CONCLUSION

For the foregoing reasons, the Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act. Consequently, we vacate the ALJ's Initial Decision and issue a Final Order requiring that LabMD notify affected individuals, establish a comprehensive information security program, and obtain assessments regarding its implementation of the program.

EXHIBIT 7

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	
	)	**Docket No. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**

ORDER EXTENDING DEADLINES FOR FILING PETITION FOR RECONSIDERATION AND ANSWER THERETO

The Commission issued the Opinion of the Commission and Final Order in this matter on July 28, 2016, and any petition for reconsideration must be filed on or before August 15, 2016. Commission Rule 3.55, 16 C.F.R. § 3.55. On August 10, Respondent LabMD filed an unopposed motion to extend the deadline for filing a petition for reconsideration by fifteen days, until August 30, and to extend the deadline for Complaint Counsel to file an answer to any such petition until September 13.

The Commission has determined, pursuant to Commission Rule 4.3(b), 16 C.F.R. § 4.3(b), to grant an extension due to the extensive and complex record in this matter and the important issues presented. We note, however, that petitions for reconsideration "must be confined to new questions raised by the decision or final order and upon which the petitioner had no opportunity to argue before the Commission." Commission Rule 3.55, 16 C.F.R. § 3.55. Because the permissible grounds for reconsideration are narrow, we believe a modest extension of one week to file a petition for reconsideration is sufficient. Accordingly,

IT IS ORDERED that any petition for reconsideration of the Opinion of the Commission and Final Order in this matter must be filed on or before August 22, 2016, and that any answer to any such petition must be filed on or before September 2, 2016.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: August 12, 2016

EXHIBIT 8

1023099

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
LabMD, Inc.,	)	**DOCKET NO. 9357**
a corporation.	)	
	)	**PROVISIONALLY REDACTED**
	)	**PUBLIC VERSION**

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that LabMD, Inc. ("LabMD" or "respondent"), a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

RESPONDENT'S BUSINESS

1. Respondent LabMD is a Georgia corporation with its principal office or place of business at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339.

2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Since at least 2001, respondent has been in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers.

4. Respondent files insurance claims for charges related to the clinical laboratory tests with health insurance companies. Insured consumers typically pay the part of respondent's charges not covered by insurance; uninsured consumers are responsible for the full amount of the charges. Consumers in many instances pay respondent's charges with credit cards or personal checks.

5. Respondent tests samples from consumers located throughout the United States.

6. In performing tests, respondent routinely obtains information about consumers, including, but not limited to: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers ("SSN"); medical record numbers; bank account or credit card information; health care provider names, addresses, and telephone numbers; laboratory tests, test codes and results, and diagnoses; clinical histories; and health insurance company names and policy numbers (collectively, "personal information").

7. Respondent has accumulated and maintains personal information for nearly one million consumers.

8. Respondent operates computer networks in conducting its business. The computer networks include computers, servers, and other devices in respondent's corporate offices and laboratory, computers used by its personnel in different parts of the country, and computers that respondent provides to some health care providers.

9. Among other things, respondent uses the computer networks to: receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to consumers; obtain approvals for payments made by consumers with credit cards; and prepare medical records. For example, respondent's billing department uses the computer networks to generate or access documents related to processing claims and payments, such as:

   (a) monthly spreadsheets of insurance claims and payments ("insurance aging reports"), which may include personal information such as consumer names, dates of birth, SSNs, the American Medical Association current procedural terminology ("CPT") codes for the laboratory test conducted, and health insurance company names, addresses, and policy numbers;

   (b) spreadsheets of payments received from consumers ("Day Sheets"), which may include personal information such as consumer names, SSNs, and methods, amounts, and dates of payments; and

   (c) copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers ("copied checks").

RESPONDENT'S SECURITY PRACTICES

10. At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

    (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;

    (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;

    (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

    (d) did not adequately train employees to safeguard personal information;

    (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;

    (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities; and

    (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks.

11. Respondent could have corrected its security failures at relatively low cost using readily available security measures.

12. Consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid possible harms from such failures, including identity theft, medical identity theft, and other harms, such as disclosure of sensitive, private medical information.

PEER-TO-PEER FILE SHARING APPLICATIONS

13. Peer-to-peer ("P2P") file sharing applications are often used to share music, videos, pictures, and other materials between persons and entities using computers with the same or a compatible P2P application ("P2P network").

14. P2P applications allow a user to both designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network.

15. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network.

16. Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.

SECURITY INCIDENTS

17. In May 2008, a third party informed respondent that its June 2007 insurance aging report (the "P2P insurance aging file") was available on a P2P network through Limewire, a P2P file sharing application.

18. After receiving the May 2008 notice that the P2P insurance aging file was available through Limewire, respondent determined that:

    (a) Limewire had been downloaded and installed on a computer used by respondent's billing department manager (the "billing computer");

    (b) at that point in time, the P2P insurance aging file was one of hundreds of files that were designated for sharing from the billing computer using Limewire; and

    (c) Limewire had been installed on the billing computer no later than 2006.

19. The P2P insurance aging file contains personal information about approximately 9,300 consumers, including names, dates of birth, SSNs, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers.

20. Respondent had no business need for Limewire and removed it from the billing computer in May 2008, after receiving notice.

21. In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. These Day Sheets include personal information, such as names and SSNs, of several hundred consumers in different states. Many of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file. A number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves.

VIOLATION OF THE FTC ACT

22. As set forth in Paragraphs 6 through 21, respondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

23. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

NOTICE

Notice is hereby given to the respondent that the twenty-eighth day of April, 2014, at 10:00 a.m., is hereby fixed as the time, and the Federal Trade Commission offices at 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580, as the place when and where a hearing will be had before an Administrative Law Judge of the Federal Trade Commission, on the charges set forth in this complaint, at which time and place you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this complaint.

You are notified that the opportunity is afforded you to file with the Federal Trade Commission an answer to this complaint on or before the fourteenth (14th) day after service of it upon you. An answer in which the allegations of the complaint are contested shall contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the complaint not thus answered shall be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the complaint, the answer shall consist of a statement that you admit all of the material facts to be true. Such an answer shall constitute a waiver of hearings as to the facts alleged in the complaint and, together with the complaint, will provide a record basis on which the Commission shall issue a final decision containing appropriate findings and conclusions, and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under Rule 3.46 of the Commission's Rules of Practice for Adjudicative Proceedings.

Failure to answer within the time above provided shall be deemed to constitute a waiver of your right to appear and to contest the allegations of the complaint, and shall authorize the Commission, without further notice to you, to find the facts to be as alleged in the complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge shall hold a prehearing scheduling conference not later than ten (10) days after the answer is filed by the respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than five (5) days after the answer is filed by the respondent. Rule 3.31(b) obligates counsel for each party, within five (5) days of receiving respondent's answer, to make certain disclosures without awaiting a formal discovery request.

The following is the form of order which the Commission has reason to believe should issue if the facts are found to be as alleged in the complaint. If, however, the Commission should conclude from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary or appropriate.

Moreover, the Commission has reason to believe that, if the facts are found as alleged in the complaint, it may be necessary and appropriate for the Commission to seek relief to redress injury to consumers, or other persons, partnerships or corporations, in the form of restitution for past, present, and future consumers and such other types of relief as are set forth in Section 19(b) of the Federal Trade Commission Act. The Commission will determine whether to apply to a court for such relief on the basis of the adjudicative proceedings in this matter and such other factors as are relevant to consider the necessity and appropriateness of such action.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

2. Unless otherwise specified, "respondent" shall mean LabMD, Inc., and its successors and assigns.

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents.

4. "Insurance File" shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network.

5. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

6. "Sacramento Documents" shall mean the documents identified in Appendix A.

I.

IT IS ORDERED that the respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and

D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099. Provided, however, that in lieu of overnight courier, assessments may be sent by first-class mail, but only if an electronic version of any such assessment is contemporaneously sent to the Commission at Debrief@ftc.gov.

III.

IT IS FURTHER ORDERED that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of service of this order unless an appropriate notice has already been provided, as follows:

A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.),

and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website (www.ftc.gov/idtheft), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from www.annualcreditreport.com and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and

3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.

B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.

C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099.

VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

IN WITNESS WHEREOF, the Federal Trade Commission has caused this complaint to be signed by its Secretary and its official seal to be hereto affixed, at Washington, D.C. this twenty-eighth day of August, 2013.

By the Commission.

Donald S. Clark
Secretary

Appendix A

EXHIBIT 9

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 10

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 11

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 12

PUBLIC

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, INC.,	)	
Plaintiff,	)	
	)	Civil Action No.: _____
v.	)	
	)	*Related Case*:
FEDERAL TRADE COMMISSION,	)	FTC v. LabMD et al.,
	)	1:12-cv-3005-WSD
Defendant.	)	

VERIFIED COMPLAINT
FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff LabMD, INC. ("LabMD") hereby states its complaint for declaratory and injunctive relief against the unconstitutional abuse of government power and ultra vires actions by Defendant Federal Trade Commission (the "FTC" or "Commission") as follows:

PARTIES, JURISDICTION, AND VENUE

1. LabMD, 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339, is a small medical cancer diagnostics business.

2. The FTC, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, is a federal agency for purposes of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 et seq.

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702. In LabMD v. FTC, Case No. 13-15267-F, at 2 (11th Cir. Feb. 18, 2014), the United States Court of Appeals for the Eleventh Circuit examined whether it had jurisdiction to entertain LabMD's claims against the FTC under the APA, as codified in relevant part at 5 U.S.C. §§ 701-06, under the federal Constitution, and under 28 U.S.C. § 1331, which allows for "nonstatutory" review of ultra vires agency actions. The Court held:

> [J]urisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted [by LabMD] at this stage, first must be asserted and considered in a district court.

(internal citations omitted). A true and correct copy of the foregoing Order is attached hereto as Exhibit 1 and is incorporated herein by reference. See also Sackett v. E.P.A., 132 S. Ct. 1367, 1373 (2012) (". . . the APA provides for judicial review of all *final* agency actions . . . ."); id. at 1374 ("The Court holds that the Sacketts may immediately litigate their jurisdictional challenge in federal court. I agree, for the Agency has ruled definitively on that question.") (Ginsburg, J. concurring). The grounds for the relief requested include the due process clause of the United States Constitution, 5 U.S.C. §§ 701-706 (APA's judicial review provisions), 28 U.S.C. §

1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), and 28 U.S.C. § 2202 (further relief).

4. The FTC has finally determined that it has jurisdiction over LabMD and that it has complied with constitutional due process fair-notice requirements: In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Jan. 16, 2014). A true and correct copy of the foregoing order is attached hereto as Exhibit 2 and is incorporated herein by reference.

5. The FTC claims the foregoing decision marks the consummation of its decisionmaking process, has the force of law, and is entitled to deference under "Chevron." See Supplemental Letter Brief, FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD, Dkt. 152-1, at 6 (Jan. 21, 2014). A true and correct copy of the foregoing brief is attached hereto as Exhibit 3 and is incorporated herein by reference.

6. Venue is proper under 28 U.S.C. §1391(e).

NATURE OF THE CASE

7. LabMD, at all relevant times a small medical laboratory providing doctors with cancer-detection services, is now on the verge of ceasing all operations after being trapped in a paralyzing web of government investigations, subpoenas, and administrative litigation.

8. At some unknown point between 2005 and August 2013, the FTC, through enforcement activities and/or internet postings on the FTC's website, rather than through administrative rulemaking, guidance or known standards, declared for the first time that certain unspecified patient-information data-security practices employed by LabMD were inadequate and thus an "unfair" trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5").

9. The FTC still has yet to issue any rule or statement with legal force and effect describing the specific patient-information data-security practices it believes Section 5 prohibits or permits.

10. Between 2005 and the present, the FTC never specified in a rule or statement with legal force and effect how LabMD's patient-information practices fell short or described what, exactly, it should have done differently at any given point. In fact, the FTC commenced an investigation of LabMD in January 2010, filed its administrative complaint in August 2013, and still today, LabMD has yet to be told what, exactly, it did wrong at any point during the relevant period of years.

11. The FTC's actions and a campaign of disparagement, including conclusory statements by an FTC Commissioner that LabMD had mishandled sensitive patient information made shortly after the administrative complaint had been filed, have eviscerated LabMD's business and destroyed its professional reputation.

12. In October, 2013, LabMD lost its directors and officers (D&O) liability insurance as a result of the pending enforcement action and has been unable to obtain D&O insurance because of the pending action.

13. Further, LabMD and its doctors were denied "tail" medical malpractice insurance because of the FTC's actions, which will, unless this matter is resolved favorably in the near future, severely limit LabMD's prospects for obtaining medical malpractice insurance going forward and thus hiring qualified physicians.

14. The company's insurance carrier has advised that it will not renew LabMD's general liability insurance policy effective May 6, 2014, so that the policy will terminate effective October, 2014. This means that LabMD cannot rent office space.

15. The FTC's actions have forced LabMD, a company that once employed more than forty people and provided diagnostic services to more than one hundred doctors, to stop accepting samples.

16. At all times relevant, LabMD's Protected Health Information ("PHI"), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act

("HITECH"), 42 U.S.C. §§ 300jj et seq., 17901 et seq. See http://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration .

17. Neither the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH. See Complaint, In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Aug. 28, 2013). A true and correct copy of the foregoing complaint is attached hereto as Exhibit 4.

18. Even if Section 5 does empower the FTC to broadly regulate data-security, which it does not, Congress delegated sole authority to regulate PHI data-security to the HHS. And even if Section 5 does empower the FTC to regulate PHI data-security concurrently with HHS and/or to "overfile" HHS using a "common law" of consent orders and internet posts to impose requirements in excess of those set through HHS rulemaking, which it does not, the Commission's refusal to promulgate rules or regulations and provide the public with proper notice and comment violates LabMD's due process rights by failing to give fair notice of what the FTC believes Section 5 forbids or requires.

19. Not only does the FTC lack the statutory authority to regulate PHI and/or cyber-security, it also lacks the expertise to do so. For example, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (Feb.

19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed Mar. 18, 2014), directed the Department of Commerce to set data-security standards, not the FTC.

20. To stop the abuse, LabMD seeks a declaration that the FTC lacks jurisdiction under Section 5 over PHI data-security practices and that the FTC has violated LabMD's due process and First Amendment rights. It also seeks preliminary and permanent injunctive relief staying the administrative proceedings in In the Matter of LabMD, Inc., FTC Dkt. No. 9357. Finally, LabMD asks that the FTC pay all of LabMD's attorneys' fees and litigation costs.

FACTS

21. Section 5 authorizes the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce."

22. The FTC in this case claims Section 5 "unfairness" authority to regulate LabMD's PHI data-security practices, even absent a claim of "deception," by way of administrative "common law" established through consent orders and Internet postings.

I. The FTC Targets LabMD.

23. In or about 2008, Tiversa Holding Corp. ("Tiversa"), a self-described "cyber-intelligence company" specializing in searching for and copying medical,

financial, and other sensitive files on peer-to-peer networks using patented technology, obtained a LabMD accounts-receivable computer file containing PHI without LabMD's knowledge or consent.

24. On May 13, 2008, Tiversa contacted LabMD, advised it that Tiversa had taken its property, and refused to provide information on the procurement of the file unless LabMD entered into a contract for Internet security services. LabMD turned down this offer. See Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012). A true and correct copy of the foregoing dissent is attached hereto as Exhibit 5 and is incorporated herein by reference.

25. In 2009, Tiversa gave LabMD's PHI accounts-receivable file to the FTC under highly irregular circumstances. See id. Recent deposition testimony of Tiversa's CEO, Robert Boback, suggests the FTC and Tiversa met on multiple occasions and ultimately conspired and agreed to transfer LabMD's file via a FTC civil investigative demand (CID) to a third company (the "Privacy Institute") that, upon information and belief, is a company that has a relationship with a Tiversa advisory board member.

26. Beginning in January 2010, the FTC requested and LabMD voluntarily provided thousands of pages of documents and submitted to multiple meetings and interviews.

27. Then, on December 21, 2011, the FTC issued formal civil investigative demands (the "CIDs") to LabMD.

28. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining, among other things, that LabMD's PHI data security was exclusively regulated by HHS and solely subject to HHS rules and regulations establishing data-security standards for PHI under HIPAA and HITECH.

29. Commissioner Julie Brill denied LabMD's petition on April 20, 2012. Commission Letter Denying LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand, in File No. 1023099, at 13 (April 20, 2012). A true and correct copy of the foregoing correspondence is attached hereto as Exhibit 6 and is incorporated herein by reference.

30. Commissioner Brill acknowledged that LabMD's PHI accounts-receivable spreadsheet file "can be considered" protected health information regulated under HIPAA and HITECH but claimed that the FTC jurisdiction under Section 5 was "overlapping and concurrent." Id.

31. On April 25, 2012, LabMD appealed Commissioner Brill's ruling, arguing, as the Commission recently admitted, that the FTC "does not enforce HIPAA or HITECH." See Ex. 2 at 12 & n.19. LabMD also challenged the FTC's reliance on the PHI accounts-receivable file obtained from Tiversa.

32. Nonetheless, on June 21, 2012, three Commissioners (including Commissioner Brill) affirmed Commission Brill's ruling, "finding its conclusions to be valid and correct." See Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD and Michael J. Daugherty (June 21, 2012). A true and correct copy of the foregoing order is attached hereto as Exhibit 7 and is incorporated herein by reference. Then-Commissioner Thomas Rosch dissented. Ex. 5.

33. The FTC then filed a petition to enforce the CIDs in this Court. LabMD opposed the petition, arguing, among other things, that the FTC lacked jurisdiction to regulate data-security.

34. The Hon. William S. Duffey upheld the CIDs, but said "there is significant merit" to LabMD's argument that Section 5 does not justify an investigation into data-security practices and consumer privacy issues. See Opinion and Order, FTC v. LabMD et al., 1:12-cv-3005-WSD, Dkt. No. 23, at 4 (N.D. Ga.

Nov. 26, 2012) (Duffy, J.). A true and correct copy of the foregoing order is attached hereto as Exhibit 8.

II. LabMD Publicly Criticizes The FTC And The FTC Retaliates.

35. LabMD's owner, Michael Daugherty decided to warn the public about the FTC's abuses through the press, social media, and a book. Mr. Daugherty used, and continues to use, his website, http://michaeljdaugherty.com/, to criticize the government.

36. For example, Mr. Daugherty was quoted in a September 7, 2012, Atlanta Business Chronicle article as follows: "'We are guilty until proven innocent with these people . . . . They are on a fishing expedition. We feel like they are beating up on small business.'" Amy Wenk, "Atlanta Medical Lab Facing Off Against FTC," Atlanta Business Chronicle (September 5, 2012). Ms. Wenk wrote that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation." Id.

37. On information and belief, FTC attorney Alain Sheer, who would later serve as lead counsel for the FTC in an enforcement action against Plaintiff, monitored Mr. Daugherty's political speech and retaliated against him for it.

38. For example, on July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his website,

http://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/. The trailer called the FTC's actions against LabMD an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming . . . [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." It criticized Commission staff, including Mr. Sheer.

39. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that the FTC commence enforcement proceedings against LabMD.

40. On July 30, 2013, Janis Claire Kestenbaum, the Senior Legal Advisor to the Chairwoman of the FTC, provided LabMD a draft complaint.

41. On August 28, 2013, the Commission commenced an enforcement action (the "Enforcement Action") by issuing a complaint and notice order. The gravamen of its claim at that time was about the PHI accounts-receivable file purloined by Tiversa. Mr. Sheer, who met with Tiversa and who was responsible for the shell-game through which the FTC obtained the file, is lead Complaint Counsel.

42. The FTC's Complaint in the Enforcement Action makes clear that LabMD was a "health care provider" and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things.

43. The FTC did not allege that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes.

44. Instead, the FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices. It said LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. See Ex. 4 ¶¶ 10-11.

45. The FTC did not name an individual complainant or allege direct harm to any person.

46. The FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively low cost."

47. The FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," allegedly violated Section 5.

48. The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security.

49. Mr. Sheer of the FTC has admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., Dkt. No. 9357, 10:11-15 (Sept. 25, 2013) ("Initial Pretrial Conf. Trans."). He also acknowledged that the FTC brought this action without any complaining witnesses who say their data was released or disclosed. Id. 33:3-5. A true and correct copy of that transcript is attached hereto as Exhibit 9.

50. No court has ever held the FTC may require firms to adopt information-practice policies under Section 5's "unfairness" prong. Hearing Trans. 16: 22-25, FTC v. LabMD, Inc. et al., Case No. 1:12-cv-3005-WSD (Sept. 19, 2012) (Duffy, J.) (emphasis added). A true and correct copy is attached hereto as Exhibit 10.

51. On September 17, 2013, LabMD filed an answer challenging the FTC's jurisdiction and violations of LabMD's federal constitutional due process rights, among other things.

52. In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.

53. On October 24, 2013, Mr. Sheer of the FTC served a subpoena duces tecum on Mr. Daugherty, LabMD's CEO and President, requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of . . . [Mr. Daugherty's book about the FTC] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" Mr. Daugherty's book about the FTC.
- "All documents related to the source material for drafts of" Mr. Daugherty's book about the FTC, "including documents referenced or quoted in the" book.
- "All promotional materials related to" Mr. Daugherty's book criticizing the FTC, "including, but not limited to, documents posted on social media, commercials featuring . . . [Mr. Daugherty], and presentations or interviews given by" Mr. Daugherty.

54. After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data-security "unfairness" offense are in this case.

55. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data-security standards—including "data-security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present."

56. Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data-security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data-security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions."

57. The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing document request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of

FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are dated after August 28, 2013, when the FTC issued this complaint. The only regulations that FTC enforcement staff produced to LabMD do not apply to LabMD and implement statutes that also do not apply to LabMD.

58. On March 3, 2014, FTC enforcement staff refused to admit, among other things, that the FTC's administrative complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5, instead claiming that LabMD was asking for "an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside of the scope of discovery" and, in the alternative, denying that they were required to allege this.

59. FTC enforcement staff have even argued that "STANDARDS USED TO ENFORCE SECTION 5 ARE OUTSIDE THE SCOPE OF DISCOVERY," saying that "[t]he orders and opinions of the Commission and of th[e ALJ] …

preclude such discovery." Complaint Counsel's Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, *In the Matter of LabMD*, FTC Dkt. No. 9357, at 7 (Feb. 14, 2014).

60. More recently, on March 18, 2014, FTC enforcement staff produced an expert witness report that for the first time—after more than four years of investigation and litigation—gave LabMD some notice as to what a FTC expert thinks LabMD did wrong. But that report did not even purport to assess LabMD's PHI data-security practices against any objective, applicable medical-industry data-security statute, regulation, custom, or standard.

III. LabMD Challenges The FTC's Jurisdiction.

61. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss raising pure issues of law and questions of statutory interpretation in the FTC's administrative case. A true and correct copy is attached hereto as Exhibit 11. LabMD requested oral argument. Under the FTC's Rules of Practice, Commissioners (and not the ALJ) rule on dispositive motions to dismiss complaints they recently voted to issue in the first instance.

62. On November 14, 2014, LabMD also filed a Verified Complaint in the U.S. District Court for the District of Columbia seeking solely injunctive and

declaratory relief. LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 1 (D.D.C. Nov. 14, 2013).

63. On November 18, 2013, LabMD filed a petition for review in the U.S. Court of Appeals for the Eleventh Circuit, LabMD, Inc. v. FTC, Case No. 13-14267-F (11th Cir. Nov. 18, 2013). Ex. 1.

64. On November 25, 2013, LabMD filed an administrative stay motion in the FTC enforcement action.

65. On December 2, 2013, LabMD filed a reply in support of its administrative motion to dismiss. A true and correct copy is attached hereto as Exhibit 12.

66. On December 13, 2013, the FTC issued an order denying LabMD's stay motion ("December 13 Order"). A true and correct copy is attached hereto as Exhibit 13. The December 13 Order states that no Article III court has jurisdiction over LabMD's claims until the FTC gives its permission.

67. On December 16, 2013, the Eleventh Circuit issued two jurisdictional questions to the parties. Jurisdictional Questions, LabMD v. FTC, Case No. 13-15267-F (Dec. 16, 2013).

68. On December 23, 2013, LabMD filed a stay motion in in the Eleventh Circuit. Petitioner's Motion for Stay Pending Review, LabMD v. FTC, Case No. 13-15267-F (Dec. 23, 2013).

69. On January 16, 2014, the FTC denied LabMD's administrative Motion to Dismiss, rejecting LabMD's jurisdictional and fair-notice due process challenges without oral argument, thereby denying LabMD an opportunity to create a record (the "January 16 Order"). Ex. 2.

70. On January 17, 2014, the FTC submitted the January 16 Order to the Eleventh Circuit, via what it called a "notice of supplemental authority."

71. FTC did the exact same thing on the exact same day in FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 151 (D. N.J. Jan. 17, 2014). The FTC claimed its order had the force of law and should be given deference under "Chevron." Ex. 3 at 6.

72. The FTC admits that it cannot and does not enforce HIPAA or HITECH. Ex. 2 at 12 & n.19.

73. The FTC admits that its case against LabMD solely alleges statutory Section 5 statutory "unfairness" violations, not "violations of the FTC's Health Breach Notification Rule." Id. at 20 n.20.

74. The FTC admits that it has failed to establish any data-security standards with the force of law that give notice as to what PHI data-security practices the Commission and its enforcement staff believes Section 5 forbids or requires. Ex. 2 at 15.

75. The FTC admits that it did not claim data-security regulatory authority until years after 1994, when Section 5 was last amended to add subsection (n). 15 U.S.C. § 45(n). Ex. 2 at 4, 8-9. Subsection (n) does not mention "data security," let alone explain what data-security practices the FTC believes Section 5 to forbid or require.

76. Yet the FTC claims subsection (n) gives fair notice: "Here, the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n) [15 U.S.C. § 45], should dispel LabMD's concern about whether the statutory prohibition of 'unfair . . . acts or practices' is sufficient to give fair notice of what conduct is prohibited." Ex. 2 at 16.

77. The FTC's January 16 Order essentially asserts that constitutional fair-notice due process requirements are somehow inapplicable here because, according to the Defendant, the FTC is not pursuing "criminal punishment or civil penalties for past conduct." Ex. 2 at 16.

78. The FTC also claims it is not obligated to provide any fair notice at all of the PHI data-security practices it believes Section 5 to forbid or require because agencies have broad "discretion" to "address an issue by rulemaking or adjudication." Ex. 2 at 15.

79. For that matter, the FTC effectively claims that the standard for Section 5 "unfairness" PHI data-security liability is whether a company's practices are "unreasonable" according to it, while acknowledging that this is a case of first impression as to what is "unreasonable."

80. Elsewhere, the FTC admitted that there is no process through which businesses could have obtained guidance or an advisory opinion from the Commission regarding data-security practices. See Hearing Trans., FTC v. Wyndham et al., Case No. 2:13-cv-01887-ES-SCM, 52:10-11 (Nov. 7, 2012). A true and correct copy of an excerpt of the foregoing transcript is attached hereto as Exhibit 14 and is incorporated herein by reference.

81. On February 18, 2014, the Eleventh Circuit dismissed LabMD's Petition for Review and denied all pending motions as moot because there was no cease and desist order reviewable under 15 U.S.C. § 45(c). Instead, it ruled this Court has original jurisdiction over LabMD's ultra vires, statutory, and constitutional claims to

the extent that such claims could be asserted before a cease and desist order is entered. Ex. 1.

82. Therefore, on February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice of LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 20 (D.D.C.), because under D.C. Circuit law, which is different from the law of this Circuit, only the U.S. Court of Appeals for the D.C. Circuit has jurisdiction over those claims, yet the D.C. Circuit will never have jurisdiction under 15 U.S.C. § 45(c) because LabMD has not done business there.

83. The FTC has issued a final agency decision regarding jurisdiction, and LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional fair-notice due process arguments.

IV. The FTC Denies LabMD Procedural Due Process.

84. To begin with, the FTC has never specified the PHI data-security standards LabMD failed to meet, thereby denying LabMD an opportunity to effectively defend itself and granting the Commission, Mr. Sheer, and other federal bureaucrats unlimited discretion to decide what is "unreasonable" after the fact and to regulate the entire health care industry based on their idiosyncratic whim, caprice, and fancy.

85. In 2009, the FTC modified its Rules of Practice to deny respondents a fair defense and to render motion practice futile. 74 Fed. Reg. 20,205 (May 1, 2009).

86. At the initial pretrial conference, the ALJ told LabMD's counsel:

> [L]et me talk about dispositive motions . . . . There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you. Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission . . . .

Ex. 9 at 18:11-15. The ALJ lacks power to even grant a continuance of the evidentiary hearing or stay the proceedings pending adjudication of dispositive motions before the Commission. See 16 C.F.R. §§ 3.22(b), 3.41(b).

87. The FTC was extensively warned about the constitutional implications of its power-grab during the comment period.

88. The American Bar Association (ABA) Section of Antitrust Law ("Antitrust Section") said the revisions forced respondents to address prehearing issues to the FTC without the benefit of a prior opinion authored by a party who was not involved in crafting and approving a complaint. Comments of the ABA Section of Antitrust Law in Response to the Federal Trade Commission's Request for Public Comment Regarding Parts 3 and 4 Rules of Practice Rulemaking—P072194, at 4 (Nov. 6, 2008).

89. The Antitrust Section explained that its "primary concern is that by 'codifying' the Commission's right to interject itself into prehearing case management, it may undermine the integrity of the process, compromise the ALJ, and create an appearance of unfairness." Id. at 12. The Antitrust Section also said the FTC's amendments "could reduce the quality of decision making, and may color the perception of the fairness and impartiality of Commission proceedings—a particularly important issue considering that when hearing an appeal, federal courts will give deference to a final FTC decision." Id. at 11.

90. The U.S. Chamber of Commerce added that "it appears that the proposed changes are being rushed into place and for the purpose of giving the FTC material, tactical, and procedural advantage . . . ." U.S. Chamber of Commerce, Comment, Re: Parts 3 and 4 Rules of Practice Rulemaking—P072104, at 1 (Nov. 6, 2008). In fact:

> The FTC's proposed regulations work to effectively eliminate the role of the independent Administrative Law Judge (ALJ) to manage and prepare an initial decision for a case. This results in the elimination of a vital check on potential unfairness inherent in the FTC's administrative procedure. Under the FTC's process, the Commissioners act as both prosecutor and judge in administrative trials. Thus, the same individuals who decide to issue the complaint also decide the final appeal of the administrative trial. With such a clear potential for unfairness or conflict of interest at the forefront of FTC administrative adjudication, it is necessary to preserve some sort of fairness check.

Id. at 2.

91. Under current Commission Rule 3.22(a), "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision shall be directly referred to the Commission and shall be ruled on by the Commission unless the Commission in its discretion refers the motion to the Administrative Law Judge."

92. In excess of their authority and in violation of the Constitution's guarantee of due process, the FTC has assumed for itself the power to legislate, to prosecute, and to judge LabMD without even specifying in advance the elements of the data-security offense LabMD has allegedly committed.

93. The empirical evidence demonstrates that the FTC's administrative process is a rigged exercise in futility for LabMD and others similarly situated.

94. According to Commissioner Wright:

> The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.

Joshua D. Wright, Comm'r, Fed. Trade Comm., Recalibrating Section 5: A Response to the CPI Symposium, CPI Antitrust Symposium, at 4 (November 2013), available at

http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last visited Mar. 18, 2014).

95. Further administrative proceedings are exhausted and futile.

V. The Irreparable Harm Done By The FTC To LabMD.

96. FTC's power-grab has destroyed LabMD's customer relationships and, in large measure, driven LabMD to cease accepting new specimen samples. But for all of the time, attention, and money LabMD has been forced to devote to addressing the FTC's actions, the company would almost certainly be accepting new specimen samples and providing cancer-diagnostic services to doctors to this day.

97. LabMD, and its doctors, have been denied insurance coverage as a direct result of the FTC's ongoing persecution of the company. For example, One Beacon (a medical malpractice insurance company) recently denied LabMD, and its doctors, coverage, saying: "[W]e are unable to offer ERP terms for the entity [LabMD], and as a result, the individual physicians so I will be closing the file. The potential volatility due to the FTC investigation is something we want to stay away from particularly because it pertains to medical records."

98. LabMD's general liability insurance carrier is planning to non-renew its insurance policy effective May 6, 2014.

99. The FTC's personnel have intentionally interfered with LabMD's customer relationships and effectively engaged in a campaign of commercial disparagement.

100. The FTC's actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace.

101. The FTC, Mr. Sheer, and other FTC employees have intentionally set out to destroy LabMD's commercial brand, reputation, and good will.

102. The FTC, Mr. Sheer, and others have caused and continue to cause LabMD irreparable harm far beyond mere litigation expenses and threaten the viability of LabMD's business operations. Much of this harm cannot be quantified in monetary terms, and cannot be remedied by monetary damages. For example, on January 6, 2014, LabMD notified its customers that it would no longer be accepting new specimen samples for testing for the foreseeable future, effective January 11, 2014.

CLAIMS FOR RELIEF

First Claim for Relief
(For Violation of the APA)

103. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 54-61, 64-66, 69-81, 84, and 93-95.

104. The FTC's action against LabMD is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right, in violation of 5 U.S.C. § 706.

105. The FTC does not have jurisdiction to regulate LabMD's patient-information data-security and thus its actions are ultra vires.

106. The Commission's orders denying the jurisdictional, ultra vires, and due process claims raised in LabMD's motion to dismiss and LabMD's motion for a stay are both "final agency actions" within the meaning of 5 U.S.C. § 704 and thus LabMD's APA claims are ripe and reviewable now. TVA v. Whitman, 336 F.3d 1236, 1248 (11th Cir. 2004); see, e.g., CSI Aviation Servs. v. DOT, 637 F.3d 408, 411-14 (D.C. Cir. 2011); see Sackett, 132 S. Ct. at 1371-72; see also Athlone Indus., Inc. v. CPSC, 707 F.2d 1485, 1487-88 (D.C. Cir. 1983).

107. LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional due-process arguments, which the Commission formally rejected on January 16, 2014.

108. In addition, only administrative remedies providing a genuine opportunity for adequate relief need be exhausted, and here exhaustion is also independently not required because the administrative process is futile and inadequate and LabMD will continue to suffer irreparable harm unless its claims are reviewed by

an Article III Court now. See N.B. by D.G. v. Alachua Cnty. Sch. Bd., 84 F.3d 1376, 1379 (11th Cir. 1996); Porter v. Schweiker, 692 F.2d 740, 742-43 (11th Cir. 1982); Randolph-Sheppard Vendors of Am. v. Weinberger, 795 F.2d 90, 107-08 (D.C. Cir. 1986) (irreparable harm excuses exhaustion).

109. Therefore, the FTC's enforcement action against LabMD should be enjoined and a declaration issued that it lacks authority to regulate patient information data-security.

Second Claim for Relief
(For Ultra Vires Agency Action)

110. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 61, 70-81, and 93-96.

111. Regardless of the presence vel non of "final agency action" under 5 U.S.C. § 704, this Court has jurisdiction to adjudicate LabMD's nonstatutory ultra vires and constitutional claims, for the presence or absence of "final agency action" has no jurisdictional effect. See, e.g., Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006); Muniz-Muniz v. U.S. Border Patrol, No. 12-4419, 2013 U.S. App. LEXIS 25400, at *11 (6th Cir. Dec. 20, 2013) (noting that "all of our sister circuits" have concluded 5 U.S.C. § 704 has no effect on a federal-question jurisdiction to adjudicate non-APA claims); see also Arbaugh v. Y & H Corp., 546 U.S. 500, 511, 516-17 (2006).

112. Thus, the FTC's ultra vires actions are ripe for judicial review now regardless of the reviewability of LabMD's APA claims.

113. Exhaustion is not required for these claims under any circumstances. See XYZ Law Firm v. FTC, 525 F. Supp. 1235, 1237 (N.D. Ga. 1981).

114. The FTC's actions against LabMD exceed the power given to it in Section 5 and are thus ultra vires.

115. Judicial review of this claim is available because the Defendant's ultra vires actions exceed the authority conferred on it by Congress and the United States Constitution.

116. Moreover, inter alia, the FTC has effectively violated three specific and mandatory restraints on its Section 5 "unfairness" power.

117. First, the FTC's abuse exceeds its delegated powers and is contrary to specific the FTC Act's prohibitions on the use of consent orders and speeches to create a binding "common law" of data security. 15 U.S.C. § 45(m)(1)(B).

118. Second, in addition to the fact that Congress has not given the FTC Section 5 "unfairness" authority to regulate data security, let alone authority to over-file HHS and regulate PHI data security, the FTC has also independently violated 15 U.S.C. § 45(n)'s specific limits on its Section 5 "unfairness" authority. 15 U.S.C. § 45(n) explicitly states that the Defendant "shall have no authority under this section

or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair" under the circumstances of this case. 15 U.S.C. § 45(n) further explicitly bars the FTC from using its public policy views as a primary basis for exercising its unfairness authority.

119. Third, the FTC's sworn responses to LabMD's discovery requests demonstrate it is seeking to enforce against LabMD random Internet postings, e-mail alerts, Commission staff reports, and congressional testimony they say establish data-security standards LabMD should have followed, even those these documents do not have the force of law and were not even published in the Federal Register, and they do not allege that LabMD had actual knowledge of any of these Internet postings and other materials. 5 U.S.C. § 552(a)(1).

120. FTC's unauthorized actions are the direct and proximate cause of LabMD's injuries, as described above. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

Third Claim for Relief
(For Fair-Notice Due Process Violations)

121. LabMD repeats paragraphs 4-5, 7-10, 46-49, 74-80, 84-85, and 118-119.

122. This Court has jurisdiction over LabMD's fair-notice due process claim now. Exhaustion is not required for these claims under any circumstances.

123. The Fifth Amendment to the United States Constitution states that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

124. The draft notice order ("Commission Notice Order") if made effective, will be in place for twenty (20) years and, inter alia, require LabMD to (1) "establish and implement, and thereafter maintain, a . . . security program"; (2) "obtain initial and biennial assessment and reports" from third parties for a period of twenty (20) years; (3) provide Commission-approved notice to the individuals listed in the accounts-receivable file and their health insurance companies of Tiversa's actions via first-class mail; (4) deliver copies of the Commission Notice Order to "current and future principals, officers, directors, and mangers," as well as deliver copies to many current and future employees, agents, representatives, and business entities; (5) notify the FTC in writing at least thirty (30) days before making numerous changes, such as change in corporate name or address; and (6) prepare and file detailed reports with the FTC.

125. Additionally, the FTC has reserved the right to order such other relief as it finds necessary and appropriate if it decides that the Commission Notice Order is insufficient, including seeking "restitution" and other types of relief authorized by Section 19 of the Federal Trade Commission Act, 15 U.S.C. § 57b (civil actions for

violations of rules and cease and desist orders respecting unfair or deceptive acts or practices), including but not limited to rescission or reformation of contracts and payment of monetary damages.

126. Under 15 U.S.C. § 45(l), each violation of the FTC cease and desist orders carries up to a $10,000 civil penalty.

127. FTC's actions, January 16 Order, December 13 Order, and the Commission Complaint and Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

128. FTC's refusal to promulgate any regulations or to issue any other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices they believe Section 5 forbids or requires, or to otherwise establish any meaningful standards, violates LabMD's due process rights.

129. Due process requires that laws that regulate persons or entities must give fair notice of conduct that is forbidden or required. FCC v. Fox TV Stations, Inc., 132 S. Ct. 2307, 2317 (2012); Connally v. Gen. Constr. Co., 269 U.S. 385, 391-95 (1926).

130. This constitutional fair-notice requirement has been thoroughly incorporated into administrative law to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. Georgia Pac. Corp. v. OSHRC, 25 F.3d 999, 1005 (11th Cir. 1994). Fair-notice due process requirements thus apply to the

FTC administrative enforcement actions seeking to impose cease and desist orders for alleged violations of Section 5.

131. The FTC has failed to meet its burden of establishing reasonably ascertainable standards for what data-security practices it believes Section 5 to either forbid or to require. See Georgia Pac. Corp., 25 F.3d at 1005; Trinity Broad. of Fla., Inc. v. FCC, 211 F.3d 618, 628-32 (D.C. Cir. 2000).

132. Basic principles of due process limit the FTC's "discretion" to enforce Section 5 through administrative adjudications; specifically, the FTC can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires. The FTC has failed to provide LabMD the baseline level of fair notice of the data-security practices it believes to be required or forbidden by Section 5's "unfairness" language.

133. Because the FTC's Section 5 PHI data-security regulatory scheme forbids or requires the doing of an act in terms so vague that men and women of common intelligence must necessarily guess at its meaning and differ as to its application, it violates due process.

134. In addition, even if the FTC's "reasonableness" standard for PHI data security otherwise passed constitutional muster, the FTC's failure to link its data-security standards to medical-industry standards independently violates due process.

135. FTC's pattern and practice of fair-notice due process violations, as applied to LabMD and all similarly situated, including the defendants in FTC v. Wyndham, violates due process.

Fourth Claim for Relief
(For Facial, Structural Due Process Violations)

136. LabMD repeats paragraphs 4-5, 7-10, 17-19, 23-34, and 84-96.

137. Exhaustion of administrative remedies is not required for facial and structural due process challenges. See, e.g., Matthews v. Eldridge, 424 U.S. 319, 329-32 (1976); Amos Treat & Co. v. SEC, 306 F.2d 260, 267 (D.C. Cir. 1963).

138. The substantial private interests affected by the FTC's actions, the high risk of erroneous deprivation of LabMD's property interests, and the high value of additional procedural safeguards outweigh the FTC's de minimis interest in the existing procedures. Therefore, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

139. Due process minimally requires a fair trial in a fair tribunal and "this applies to administrative agencies which adjudicate as well as to courts." Withrow v. Larkin, 421 U.S. 35, 46-47 (1975).

140. FTC's modifications to its Rules of Practices transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions and deprive

all respondents of a fair administrative hearing. Therefore, the Commission's Rules facially and structurally violate due process.

141. Furthermore, the FTC's ex post facto enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the FTC acts in a legislative, prosecutorial, and adjudicative capacity further violates due process.

142. Finally, the FTC has predetermined this matter, denying LabMD its right to a fair and level review, including a fair hearing on its Motion to Dismiss before an impartial ALJ.

143. FTC's intentional violations of LabMD's due process rights has caused LabMD hundreds of thousands of dollars in actual damages, harmed its business reputation, caused it to lose good will and business opportunities, and brought the company to the brink of ruin.

Fifth Claim for Relief

(For Retaliation Against LabMD for Protected First Amendment Speech)

144. LabMD repeats paragraphs 4-5, 7-11, 23-49, and 53.

145. The First Amendment to the United States Constitution guarantees LabMD freedom of speech.

146. Mr. Daugherty's book, his webpage about the book, and his speeches and statements about the FTC's actions are political speech and speech about matters of public concern and thus protected by the First Amendment.

147. On information and belief, the FTC's actions against LabMD were retaliation for protected speech by Mr. Daugherty.

148. The FTC's actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity.

149. On information and belief, the FTC's conduct herein was precisely intended and designed, at least in part, to punish LabMD and chill government criticism by LabMD and others targeted by the government.

150. Even if the FTC, Complaint Counsel, and other FTC employees disagree with and find Mr. Daugherty's statements about their actions to be patently offensive, they are not allowed retaliate by bringing an enforcement action against LabMD.

RELIEF REQUESTED

WHEREFORE LabMD requests the following relief:

A. That the Court enter a declaratory judgment that (1) the FTC lacks statutory authority to regulate patient-information data-security practices under Section 5; (2) the FTC's efforts to regulate patient information are ultra vires; (3) the FTC violated LabMD's due process rights by failing to provide constitutionally

adequate notice of what data-security practices the Commission believed Section 5 to forbid or require before the Complaint was filed; (4) the FTC violated LabMD's due process rights by unconstitutionally combining legislative, prosecutorial, investigative, and adjudicatory functions by, among other things, allowing FTC Commissioners to rule on dispositive motions concerning complaints they recently voted to issue; and (5) the FTC unconstitutionally retaliated against LabMD for engaging in constitutionally protected speech.

B. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall take no further actions in connection with administrative proceedings known as In the Matter of LabMD, FTC Dkt. No. 9357, including but not limited to issuing orders, holding hearings, taking discovery, and filing motions.

C. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall not (1) initiate any civil or administrative enforcement action against LabMD or any other person on the ground that their patient information data-security practices are "unfair" in violation of Section 5; (2) investigate whether LabMD's or any other person's patient

information data-security practices violate Section 5 for "unfairness"; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in civil or administrative proceedings; or (4) undertake or pursue any administrative enforcement proceedings until the Commission amends its Rules of Practice to provide constitutionally adequate due process.

D. That the Court award LabMD its attorneys' fees and litigation costs under the Equal Access to Justice Act and/or such other applicable law.

E. Such other and further relief as this Court deems just and proper.

Respectfully submitted, this 20th day of March, 2014.

/s/ Ronald L. Raider

Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone (404) 815-6500
Facsimile (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

Counsel for Plaintiff

OF COUNSEL:

Reed D. Rubinstein
(applying for admission pro hac vice)
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
reed.rubinstein@dinsmore.com

Senior Vice President for Litigation and
Counsel to Cause of Action

Michael D. Pepson
(applying for admission pro hac vice)
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court
and administrative proceedings before
federal agencies.

Dated: March 20, 2014

Verification

I am Michael Daugherty, owner and CEO of LabMD, Inc., which is the plaintiff in this action.

I have read the foregoing Complaint and verify and declare on behalf of LabMD, Inc., under penalty of perjury, that its factual allegations are true, except to those matters stated on information and belief, and as to those matters I believe them to be true to the best of my knowledge.

LabMD, Inc.

By: _____ Date: 3/19/14
Michael Daugherty

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14 point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: March 20, 2014.

/s/ Ronald L. Raider
Ronald L. Raider

EXHIBIT 13

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 14

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of	)	
	)	
LabMD, Inc.,	)	Docket No. 9357
a corporation,	)	
Respondent.	)	

REBUTTAL EXPERT REPORT OF CLAY SHIELDS, PH.D.

TABLE OF CONTENTS

I. Introduction 1

II. Summary of Experience and Qualifications 2

III. Overview of the Operation of Peer-to Peer Networks and Programs 5

A. A Simple Overview of Gnutella/LimeWire Operation 5

B. Search in Gnutella 7

C. Browsing in Gnutella 9

IV. Materials Considered in Forming Opinions 10

V. Rebuttal to the Expert Report of Adam Fisk 11

A. Most Likely, the 1,718 File was Inadvertently Shared to the P2P Network 11

B. Dangers of Inadvertent Sharing on P2P Networks 12

C. Searching Using LimeWire/Gnutella Functionality 16

i. Browsing 17

ii. Searches for Misconfigured P2P Peers 19

iii. File Extension Search 20

D. Searching Outside the Gnutella Mechanism 23

i. The Challenge of Creating Custom Search Software 26

ii. Crawling versus Sharing 29

E. Other Avenues of Information Disclosure 30

VI. Conclusion 31

APPENDIX A 1

APPENDIX B 2

REBUTTAL EXPERT REPORT OF CLAY SHIELDS, PH.D.

I. Introduction

1. I am a tenured full Professor in the Computer Science Department at Georgetown University, with expertise in networking and network protocols, computer security, digital forensics, and responding to network and computer system events.

2. The FTC has engaged me to testify as a rebuttal expert in this litigation. Complaint Counsel has asked me to review the report of Adam Fisk and provide opinions about Mr. Fisk's conclusions concerning the LimeWire peer-to-peer file sharing program and the disclosure of a LabMD file containing sensitive information about approximately 9,300 individuals on a peer-to-peer file sharing network (this file is known alternatively as the "insuranceaging_6.05.071.pdf" file and the "1,718 File"). In particular, as explained in more detail in Section V below, Complaint Counsel has asked me to:

a. Explain generally how peer-to-peer (p2p) networks and programs work;

b. Provide an opinion responding to Mr. Fisk's discussion of how the 1,718 file was made available to the Gnutella p2p network;

c. Evaluate Mr. Fisk's opinion that limitations of LimeWire's search functionality made it "extremely unlikely" that a typical LimeWire user could have found the 1,718 File and downloaded it from LabMD;[1]

d. Evaluate Mr. Fisk's opinion that "casual LimeWire users" could not find the 1,718 File using other methods and that only "sophisticated organizations capable of

[1] Fisk Report, p. 16, 23.

deploying the financial and ultimately technical resources required" could locate the 1,718 File;[2] and

e. Evaluate Mr. Fisk's opinion that a thumb drive or email was likely to have been used to transfer the 1,718 File to a computer outside LabMD, from where it was downloaded to a p2p network.[3]

3. Based on my review of Mr. Fisk's report, materials contained therein, and the materials described in Section IV, below, and my experience described in Section II, below, I conclude that the 1,718 File was most likely shared inadvertently and disagree with certain of Mr. Fisk's opinions. In Section V, below, I present my specific opinions that support my conclusion.

4. This report states my opinions and provides the justifications for those opinions. It includes the following information:

a. A summary of my experience and qualifications (Section II);

b. An overview of the operation of peer-to-peer networks and programs (Section III);

c. A description of the materials that I considered in forming my opinions and conclusions (Section IV); and

d. My evaluation of some of Mr. Fisk's opinions (Section V).

II. Summary of Experience and Qualifications

5. I have over 20 years of computer science experience, including my time spent earning Ph.D. and Master's degrees in Computer Engineering from UC Santa Cruz. Prior to that, I earned a bachelor's degree in Electrical Engineering from the University of Virginia. My Ph.D. dissertation was in the area of computer networking as well as network and computer security, and I have since become involved in digital forensics research, the goal of which is to improve

---

[2] Fisk Report, p. 25.
[3] Fisk Report, p. 25.

manager used LimeWire to share music files.[5] If an outside LimeWire user searched for and found a particular music file or, for example, the "W-9 Form" file in the LimeWire sharing folder on the LabMD computer used by the billing manager, the outside user could view all the other files in the sharing folder without any further searching. As Exhibit CX0152 shows, the 1,718 File is included in the LimeWire sharing folder on the billing manager's computer. The outside user could open and download any of the other folders in the sharing folder.

31. This feature allows a more general approach to discovering files of interest inside the Gnutella network. Users can look through the shared folders of other users that have collections of files that match their interests. If one file of some particular type is identified through search, a user might find it worthwhile to browse the other user's files to see if anything else of interest is available.

IV. Materials Considered in Forming Opinions

32. In reaching my opinions, I have considered: Mr. Fisk's report and materials included therein; my long experience in computer networking and digital investigations; contemporaneous security references; academic papers about p2p networks and the experiments researchers have conducted on them; and a copy of the LimeWire source code for version 4.16.6. A list of all of the materials that I considered in reaching my opinions is attached to this report as Appendix B.

33. Based on any new information that is relevant to this litigation that comes to my attention subsequent to the submission of this report through depositions or otherwise, I reserve the right to supplement my opinions as I find appropriate.

---

[5] See Deposition of Alison Simmons, February 5, 2014, p. 100; Deposition of John Boyle, January 28, 2014, p. 62.

V. Rebuttal to the Expert Report of Adam Fisk

34. I have reviewed the report of Adam Fisk. Complaint Counsel has asked me to provide opinions about Mr. Fisk's conclusions reached in this report concerning LimeWire and the 1,718 File. In this section I address several of Mr. Fisk's conclusions in turn.

A. Most Likely, the 1,718 File was Inadvertently Shared to the P2P Network

35. Complaint Counsel has asked me to provide an opinion responding to Mr. Fisk's discussion of how the 1,718 File was made available to the Gnutella p2p network. As discussed below, I conclude that the file's availability was likely inadvertent and the result of user error.

36. In his report on page 23, Mr. Fisk describes the steps that would be required to expose the 1,718 File on the network using LimeWire. He writes that Ms. Woodson (LabMD's billing manager):

a. "Installed LimeWire on her computer even though it clearly violated company policy

b. Actively chosen to share her My Documents folder, which LimeWire did not share by default

c. Actively saved the insuranceaging_6.05.071.pdf file in that folder."

37. These steps are essentially correct. Someone did install LimeWire, though I cannot offer an opinion as to whether doing so violated company policy. Someone did choose to share the "My Documents" folder, possibly even in face of warnings about the security risks of doing so. And somebody did place the 1,718 File in that folder where it would be shared. It seems reasonable to assume it was Ms. Woodson who did so.

38. It would be incorrect, however, to conclude from the evidence that she did so with the purposeful intent of sharing the file on the Gnutella network. Using a commonly-used directory

such as the "My Documents" folder for file sharing was then and is still a known problem and in fact appears common enough that LimeWire added a warning to notify users when this was happening. That Ms. Woodson likely placed the 1,718 File in her My Documents directory is not indicative of any particular intention to share it. That directory was a default location commonly offered by programs as a location to place files. In the absence of any evidence of her intentions, the most likely reason that LimeWire was sharing that directory and that the 1,718 File was there was simple user error.

B. Dangers of Inadvertent Sharing on P2P Networks

39. Running a p2p protocol is like advertising that anyone can come and take things from your garage. This doesn't present problems as long as you intend for things in the garage to be taken, but should you leave sensitive or valuable things in your garage, this can go quite wrong. The garage in this analogy is the folder of shared items on the computer. Another danger is that the user will specify the wrong folder to share, in effect allowing anyone to take things from perhaps the whole house instead of just the garage.

40. The security risks of p2p software, including inadvertent file sharing, have been known since the early 2000s. While we don't have access to a time machine to revisit that time, it is possible to find contemporaneous documents that describe the risk. Many examples come from the SANS Reading Room. SANS is the System Administration, Networking, and Security Institute. It is a well-respected organization dedicated to training systems administrators who operate and maintain computer systems and networks in the practice of security. SANS materials are a prime resource for information technology practitioners. Its advanced students produce papers on security topics which are then made publicly available on the SANS website. Looking

back at papers shows many that described the risks of p2p software at the time. I quote a few below.

41. Once such paper, titled "Peer-to-Peer File-Sharing Networks: Security Risks" was written by William Couch and contributed to the SANS reading room in 2002.[6] He wrote:

> "Another real danger of P2P networks is that, although theoretically the user controls what subdirectories he/she makes available to peer users, sometimes more subdirectories are shared than is known or intended." (p. 6).
>
> And:
>
> "Therefore, it is up to users, and security administrators, to be aware of the risks implicit in this wide-open architecture. The safest course of action is to not use, or allow, P2P file-sharing software." (p. 11)

42. About the same time, another student, Kelvin Choi, contributed a paper titled "Security Implications of "Peer-To-Peer" Software" dated July, 2004.[7] In it, he writes:

> "File sharing applications such as this present multiple exposure opportunities for the enterprise. Issues of intellectual property are paramount. Companies bear some measure of liability for employees trading and storing copyrighted works in the office. Equally distressing is the opportunity for unintentionally sharing proprietary or delicate information through carelessly or improperly configured clients. Allowing documents to be shared without explicit permissions is an easy mistake for the unwary user, and users have been known to unintentionally share entire disc volumes. This "information leakage" could be the most expensive security issue faced by the enterprise, as it has can have [sic] the greatest legal liability. This is exacerbated when employees install and configure file-sharing software outside a defined security process and infrastructure." (p. 4)

43. Similarly, Lucas Ayers wrote in a paper titled "Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications" which is dated December 20, 2003:[8]

> "It appears most of the sharing of personal files is due to user error – where a user mistakenly shares documents they didn't mean to. While this is not a true technical issue like firewall rule sets or router access lists, it is very much a Security issue. Informing users about security and making everyone aware of the

---

[6] See https://www.sans.org/reading-room/whitepapers/policyissues/peer-to-peer-file-sharing-networks-security-risks-510.
[7] See http://www.giac.org/paper/gsec/2016/security-implications-peer-to-peer-software/103490.
[8] See http://www.giac.org/paper/gsec/3519/security-ramifications-peer-peer-p2p-file-sharing-applications/105733.

> consequences of their actions, is one of the most imports tasks any security office has.
>
> There are also issues with the wizards and setup programs of some of these file sharing applications used during installation. The wizards will ask the user if they want to search for the location of typical files people share. If you happen to have a bunch of music files located in your "My Documents" folder (this is a typical location people have personal files on their computers), the setup program will share that whole folder with the rest of the P2P network. Not just the music you meant to share, but everything in that folder!" (p.13)

44. Again in 2003, Stephen Farquhar contributed a paper, titled "Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment," in which he writes:[9]

> "Sharing the File Server in one easy step - Astute users will selectively share files, but many users accept application defaults or blindly tick the first checkbox they see. This can result in the entire contents of their hard drive being shared or worse, all drives including network drives to be shared. Hence, unwittingly exposing the contents of the corporate file server to the public becomes a minor task." (p. 7)

as well as:

> "The task of preventing the use of P2P applications in the corporate environment is a subset of the task of preventing any unauthorised software usage and starts with policy, followed by a variety of techniques to form multi-layered defences." (p. 14)

45. These early works show that there was an awareness of computer security professionals that p2p networks provided a large risk, in no small part because a user could allow sharing of proprietary or confidential corporate documents.

46. This knowledge was not confined to SANS students. By 2005, there were warnings available through the US Computer Emergency Readiness Team about p2p networks.[10] It is possible to see a snapshot of a web page from that period through the Internet Archive Wayback Machine, which has been taking and preserving occasional snapshots of sites around the Internet

---

[9] See http://www.giac.org/paper/gsec/3123/peer-to-peer-p2p-file-sharing-applications-threat-corporate-environment/103882.

[10] The United States Computer Emergency Readiness Team (US-CERT) is a government agency leading efforts to "improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment." See http://www.us-cert.gov/about-us.

over a long period of time. One such web page is at:

http://web.archive.org/web/20051127091241/http://www.us-cert.gov/cas/tips/ST05-007.html.

This page, captured in November 2005, but marked as updated in June 2005 reads in part:

> "**Exposure of sensitive or personal information** - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft (see Protecting Your Privacy and Avoiding Social Engineering and Phishing Attacks for more information)."

47. By 2005, various organizations had warned about the risk of inadvertent file sharing through p2p programs, and by 2006, concern about p2p networks and defending against security problems they had caused had reached the state of best practice. As seen in the document "Security Best Practices", written by Dr. Eric Cole (a security consultant and SANS instructor):[11]

> "The most important security practice, that which all other security controls and protections are based on, is the creation and enforcement of security policies. Every organization must have an overall policy that establishes the direction of the organization and its security mission as well as roles and responsibilities. There can also be system specific rules to address the policies for individual systems and data. Most importantly, the appropriate use of computing resources must be addressed. In addition, policies can address a number of security controls from passwords and backups, to proprietary information. There should be clear procedures and processes to follow for each policy. These policies should be included in the employee handbook and posted on a readily accessible intranet site.
>
> The organization's security policies should address applications, services and activities that are prohibited. These can include, among others, viewing inappropriate material, spam, **peer-to-peer file sharing**, instant messaging, unauthorized wireless devices and the use of unencrypted remote connections such as Telnet and FTP. Appropriate use policies should outline users' roles and responsibilities with regard to security. They should provide the user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If an organization identifies specific actions that could

---

[11] See http://www.securityhaven.com/docs/Security_Best_Practices.pdf.

> result in punitive or disciplinary actions against an employee, these actions and ways to avoid them should be clearly explained in the policy." (p. 2, emphasis added)

48. The fact that inadvertent sharing of sensitive documents was a concern and needed to be prevented by specific policy, procedure, and training was well known among information technology practitioners by 2006. By 2005, other organizations were warning about risks presented by p2p programs to more general audiences.[12]

49. For the reasons set out above, p2p programs presented a well-known and significant risk that files would be inadvertently shared. Because the LimeWire sharing folder on the LabMD computer used by the billing manager included hundreds of files, including music files and .pdf files, it is likely that the 1,718 File was inadvertently included in the sharing folder.[13]

C. Searching Using LimeWire/Gnutella Functionality

50. Complaint Counsel has asked for my opinion about Mr. Fisk's conclusion about the ways by which the 1,718 File could have been found and copied from the LabMD computer of Rosalind Woodson, LabMD's billing manager, using LimeWire. As I explain below, I believe there are other ways the 1,718 File could be found besides the exact file name search Mr. Fisk identifies.

51. Mr. Fisk makes the point that it would be difficult for a searcher to create a search that would find the file named "insuranceaging_6.05.071.pdf" on pages 11-13 of his report. He states that the searcher would have to enter either the term "insuranceageing" or "6.05.071" in order to find the file.

52. Mr. Fisk concludes that "it is extremely unlikely that any *typical* user of the Gnutella network, including highly sophisticated users, would ever have found the

---

[12] See, e.g., http://www.ftc.gov/news-events/press-releases/2005/06/ftc-issues-report-peer-peer-file-sharing.
[13] Mr. Fisk presents no evidence to support his alternative hypothesis that the file was shared by email or portable media, which I discuss in Section D, below.

"insuranceaging_6.05.071.pdf" file in question using search alone."[14] He also concludes that "only extremely sophisticated and custom-designed software would ever be configured in this fashion," meaning in a way suitable for locating the 1,718 File.[15]

53. Mr. Fisk reaches his conclusion in part based on an unreasonable assumption about how the file could be found, ignoring a variety of other methods that would account for its eventual exposure through LimeWire.

54. His conclusion addresses only one very narrow possibility of how the file might have been discovered through the Gnutella network, which is searching for it based on its exact name.[16] This conclusion is almost certainly incorrect as there is at least one search method that could return the file without using either of the two file name terms Mr. Fisk identifies.

55. More importantly, he does not conclude that the 1,718 File was not downloaded using the LimeWire program that was indisputably sharing the file. His report instead hints at a number of ways that it could have happened, and he addresses and rules out none of them.[17] There are viable ways that the file could have been found and copied from the LabMD system and I describe below three simple, relatively unsophisticated methods, other than using the two file name terms Mr. Fisk identifies, by which the 1,718 File could have been retrieved through LimeWire.

i. Browsing

56. LimeWire contains functionality that allows any user of the network to connect directly to another computer running LimeWire. Once connected, the user can see all files that are

---

[14] Fisk Report, p. 16.
[15] Fisk Report, p. 24.
[16] Fisk Report, p. 13.
[17] Fisk Report, pp. 24-25.

available for download. This information is most often presented as a list that the user can scroll through, and should the user choose to, he or she can click on any file and download it directly.

57. The simplest way this "browse host" functionality might have been used to download the 1,718 File is for a user to have received a search hit for some other file that was present on the LabMD computer running LimeWire, and then chosen to use the "browse host" function to examine and download other files from the computer. My understanding is that Ms. Woodson was using LimeWire to download and share popular music that could result in many search hits. This could easily have led to the 1,718 File being downloaded through browse host.

58. In addition, the shared folders on Ms. Woodson's computer contained other files that might have drawn the interest of potential thieves and could have been found through the basic search. For example, there was a file named "W-9 Form" being shared.[18] A person who was interested in identity theft might have been searching on that term to find addresses and Social Security numbers. The browse host function could then be used to view and download the 1,718 File that was contained in the same shared folders.

59. While it may be unlikely that any random user would choose to download the 1,718 File, this low probability must be balanced against the enormous number of users on the Gnutella system. An analogy is the Powerball lottery. The chance of any one ticket winning is low, but given that so many people buy tickets the lottery is won relatively frequently.

60. Mr. Fisk, on page 15 of his report, states:

> "At any one time on the LimeWire network there would be approximately 2 to 5 million users online."

---

[18] Citizens use the Internal Revenue Service's W-9 Form to request a taxpayer identification number. In completing the form, citizens enter, among other things, their names, addresses, and Social Security numbers. Internal Revenue Service, "Request for Taxpayer Identification Number and Certification" (November 2005), *available at* http://dese mo.gov/se/documents/se-fs-w9.pdf.

61. Over an extended period of time, such as weeks or months, even a 1 in 1,000,000 chance of someone downloading the 1,718 File would therefore result in it being downloaded many times. It takes only one such download to allow the information to be released.

62. Mr. Fisk also goes into detail describing the LabMD firewall's operation, but also implies that the firewall would not have prevented the "browse host" feature from being used when he states on page 16:

> "In order to download the files of a browse host either the Downloader or the Uploader must not be behind a firewall."

63. While the LabMD computer was behind a firewall, any computer that itself was not behind a firewall could therefore have used the browse host function to download the 1,718 File.

ii. Searches for Misconfigured P2P Peers

64. Above, I discussed the possibility that a random user found and downloaded the 1,718 File from the LabMD computer through LimeWire using the "browse host" function. There is a more deliberate way that the file could have been found and downloaded.

65. The Internet, being a public network, is sometimes used by people who might have fraudulent or malicious intent, including those looking for sensitive documents that p2p users did not intend to share. One opportunity for them to get documents is to identify and exploit misconfigured p2p nodes that are likely to expose sensitive information, then to download and make use of that information. Notably, these actors do not need to have any information about the names of the files they hope to find. Instead, they gather open information about common files that are placed in particular directories when installed. For example, they can search for particular operating system files that appear under the directory C:\windows, or common files installed by applications that are placed in the "My Documents" folder. A badly mis-configured

Windows XP node that was sharing its C: drive would be easily identifiable by searching for a file named Zapotec.bmp, which is a default file included in that version of Windows.

66. Finding one of these files would signal a high probability that the LimeWire program on a computer was misconfigured and was currently exposing files in the directory where files like the 1,718 File are normally found. For example, a file known to be installed in "My Documents" that was found as a result of a search would indicate that that computer was exposing the "My Documents" folder, which is likely to contain a large number of files of various types. The person would then connect to that computer and use the "browse host" functionality to download and examine potentially interesting files that were exposed.

67. The LabMD computer, which was running LimeWire, would have been vulnerable to being found in this manner. Unfortunately, LabMD produced incomplete information about which files were being shared so it is difficult to identify which files might have been the lure to attract someone who was actively seeking misconfigured peers. Nevertheless, the fact that the information was being made publicly available on a network known to be used by malicious actors means that there is a reasonable possibility the file could have been discovered in this manner.

iii. File Extension Search

68. As noted above, Mr. Fisk writes extensively to make the case that it would be difficult for a searcher to find the 1,718 File using its filename.[19]

69. I believe he is mistaken, and there is one simple and direct search that would return that file, which is to search on the portion of the filename he neglects – the file extension "pdf."

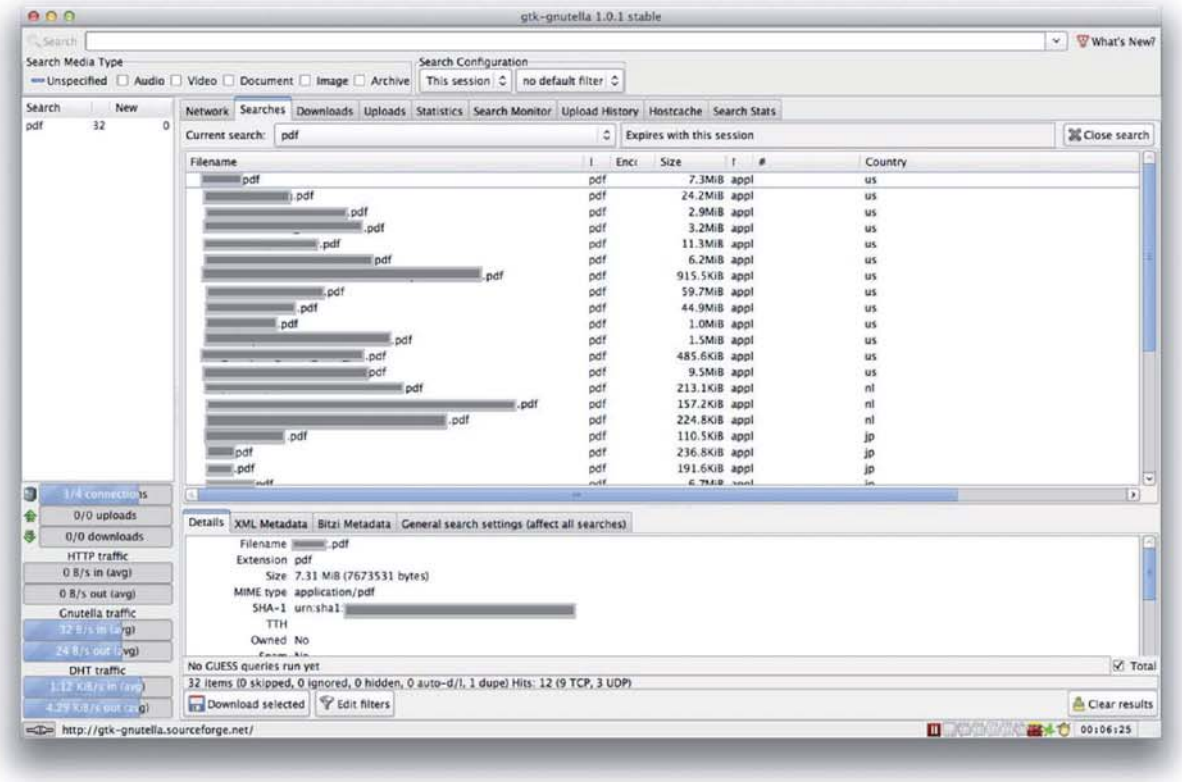
---

[19] Fisk Report, pp. 13-16, 23.

70. The file extension "pdf" indicates that the file is formatted as an Adobe Portable Document Format (PDF) file. This format is commonly used for documents that contain text and images, but which are not intended to be edited. It is very commonly used in academic and business environments for distributing documents. I have also encountered entire books being formatted and shared as PDF files.

71. Gnutella users who are searching the network might then choose to search for PDF if they had interest in those types of documents. Such a search would easily return the 1,718 File. To demonstrate that this is possible and easy to do, I performed searches with the current Gnutella network using the "gtk-gnutella" program and verified that a search using the term "pdf" returns search results that consist of PDF files, the bulk of which contain the string "pdf" only in the file extension. The image below shows the results of such a search using the gtk-gnutella program, version 1.01 available from http://gtk-gnutella.sourceforge.net/ and the files it returned.[20]

[20] Files names except for extensions have been redacted in the image.



72. The question then becomes "Did LimeWire support this type of search during the relevant period?" Unfortunately, LimeWire was ordered closed, and at that point we lost full access to the site containing the source code and documentation.[21] We do, however, have some remnants of the LimeWire site as recorded by the Internet Archive Wayback Machine.

73. Searching using the Wayback Machine allowed me to retrieve a copy of the LimeWire source code for version 4.16.6, which was similar to the version that was running on the LabMD computer Rosalind Woodson used.[22] It was the closest version to the version 4.16.7 on the LabMD computer that the Wayback Machine had archived, and is very close to the code running

---

[21] *Arista Records, LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 96 U.S.P.Q 2d 1437 (S.D.N.Y 2010).
[22] I downloaded this code from the URL: http://web.archive.org/web/20081203173114/http://www.limewire.org/limewire.zip.

on the LabMD computer, judging from the version number. I examined the code of the program to determine if file extensions, such as ".pdf" were excluded when searching with LimeWire.

74. I found no such code. Instead, I found code that supports the theory that LimeWire allowed searches by file extension and then returned files containing that file extension. In the file from the source code distribution named GreedyQueryFilter.java, there is code to limit searches that would be excessively burdensome on the Gnutella network. The code in question is named `isVeryGeneralSearch`, lines 43-65. I will spare quoting the code in detail, but the comment describing the code is accurate as to its functionality and reads:

a. "Search through a query string and see if matches a very general search such as "*.*", "*.mp3", or "*.mpg" and check for uppercase also"

75. This shows that the code blocked searches based on the file extensions ".mp3" and ".mpg", which are for music and audio files and movie files, respectively. This strongly implies that searches based on file extensions were possible, and that those searches for PDF files were not blocked. Assuming the implication is correct, file extension searches were possible in LimeWire and would have returned the 1,718 File.

76. Again, this indicates that users who were searching for the types of documents that are commonly found in businesses, such as Microsoft Office documents and PDF files, could have easily found the 1,718 File using search without using any more specific terms.

D. Searching Outside the Gnutella Mechanism

77. Complaint Counsel has asked me to provide an opinion about Mr. Fisk's conclusion that only "sophisticated organizations capable of deploying the financial and ultimately technical resources required" to write and use custom search software to crawl p2p networks could locate the 1,718 File. These programs would be written to make use of the protocol mechanisms to

traverse the network to catalog its participants and the names of content they were sharing instead of downloading code. As I explain below, creating such software is not limited to "sophisticated organizations."

78. Mr. Fisk first makes the incorrect assumption that the 1,718 File had to have been found by searching exactly for either of the two file name terms he identifies.[23] As discussed above, this assumption is incorrect as it was entirely possible for the file to be located without searching by either of file name terms Mr. Fisk identifies. Following from this first incorrect assumption, he then states that the only way for this document to have been located on the Gnutella network was through custom search software, implying that this software must have used the "browse host" function to search through files on all hosts.[24] He then uses the assumption of custom software to state that only a "sophisticated" organization with large financial and technical resources could write such code, and that such code indicates knowledge no normal network user would have.[25] Finally, he suggests that the other copies of the 1,718 File located on LabMD's network were therefore found by and later shared by one of these organizations.[26]

79. This chain of logic is almost entirely incorrect. Custom search software using the "browse host" function is not difficult to create, as most of the code needed already exists and is freely available. It would require little specialized knowledge of the protocol as the code available already encodes protocol knowledge. Because the code is readily available, almost anyone with the necessary undergraduate-level programming experience could create it, and a brief search finds evidence that this has happened. The organizations that Mr. Fisk suggests might have created such software also have incentives not to share what they might find, and it is

---

[23] Fisk Report, p. 13.
[24] Fisk Report, p. 24.
[25] Fisk Report, pp. 24-25.
[26] Fisk Report, pp. 24-25.

unlikely, had they downloaded any files from the network, that they would have then shared them.

80. Mr. Fisk's argument makes the following points:

a. Implicitly, he assumes that the file can only be found by searching for it using its filename.

b. He then claims that no ordinary user could have found the 1,718 File using normal search.

c. As search must have been used, but normal search would not have worked, then the person who found it must have written their own search.

d. This search must have used the "nuances" of the "browse host" functionality.

e. No ordinary user could or would write their own search this way; they would not have the technological resources to do so.

f. Therefore, it must have been an organization like Tiversa, the FBI, Big Champagne, or the RIAA.

g. Because the file was later found at multiple IP addresses online, it is possible that it was then being shared by the organizations above who had created their own search software.

81. I have addressed points a and b in Section A above. There is no need for the file to have been found only by searching for its filename. It could have been randomly browsed, found as part of a search for misconfigured peers, or found by searching for the term "pdf," as I explained above. Below I address his custom search argument (points c, d, e, and f).

i. The Challenge of Creating Custom Search Software

82. Though it is clear that writing a custom search was not necessary, I would like to address the points c, d, e and f regarding writing custom software. Mr. Fisk is incorrect in most particulars. Writing such software is not challenging, as most of the code exists and embeds the necessary knowledge of the protocol. It might take only someone with an undergraduate computer science degree and basic networking knowledge, and there is evidence that this has happened.

83. First, Mr. Fisk is not very precise in defining what constitutes an "ordinary user." There are distinctions that need to be made in discussing what a *user* of p2p software can do with the software, and what a *developer* who is extending p2p software can make the software do in accordance with the Gnutella protocol. In the first case, an "ordinary user" would be one who uses an existing p2p software client, like LimeWire. They would be limited to the functionality that was built into the software by the developers. In LimeWire, these are things like search, download, and browsing a host where you have located a file.

84. The developer of the software, however, has access to all the functionality that the Gnutella protocol provides. This is more functionality than is commonly built into the software. The reason is that the protocol provides a variety of possible services which are generally used in one way, say to provide normal search and download services, but which can be recombined in a different way, say to create a browse-based search, in a way that does not violate the operation of the protocol. In the example of a browse-based search, the developer would choose to combine the portion of the protocol that does peer-discovery with the portion of the protocol that allows host browsing to extract the information of what files are in the network. The developer could then create his or her own index and search across that. Such activity is normal or ordinary from the point of view of the other participants of the protocol.

85. Second, Mr. Fisk implies that creation of this software is something that is out of reach of the average developer. He states (page 24):

> "The vital point is that only extremely sophisticated and custom-designed software would ever be configured in this fashion"
>
> and (page 24, again):
>
> "In order to find the 1,718 File someone would have to understand the nuances of the browse host message and would have had to have written custom software to take advantage of that knowledge."

86. This implication is not the case. A programmer who wanted to create software that took advantage of the Gnutella network can draw on a publically available and well-documented code base that would provide most of the functionality needed.

87. As I am fond of explaining to my programming classes, programmers are lazy – but they are lazy in a good way, which means doing as little work as possible to achieve whatever programming goal they are trying to reach. This often is demonstrated by the reuse of existing code. It is generally faster and easier to find code that does what you want than it is to write it yourself. In fact, code reuse is highly encouraged in the computer science community, and languages like Java include a concept called "classes" which allow ease of code reuse.

88. To support code reuse, there are often practices to help generate documentation as code is written, so that other programmers can more easily understand the existing code. Java uses a system called "javadocs" that allows programmers to annotate their code, and then to later use the annotations as the input to a program that converts them to readable documentation.

89. LimeWire itself is written in Java, and uses javadocs to create documentation. There are other Gnutella clients available as well, and a programmer who wanted to extend the Gnutella

functionality could download the source code of the programs and use that as a basis for this work. This would greatly increase the ease and speed of developing code that works with the Gnutella protocol.

90. Using existing code for Gnutella removes the need for programmers to completely understand all aspects of the Gnutella protocol, as the Java language classes already written encapsulate the knowledge of the original programmer. Others can then use the interface in the class to interact with Gnutella without needing full knowledge of how the protocol works. This removes the need for other programmers to understand all the details of the protocol.

91. Most networking code is written in this way. Networking code is divided into a series of components, known as the "networking stack." Each layer of the stack provides an interface that enables functionality without requiring deep protocol knowledge, so reusing Gnutella code would be a natural extension of this approach.

92. To see if there was evidence to support the idea that large-scale cataloging of files that were available on Gnutella through the browse host function was not as challenging as Mr. Fisk indicates, I did a brief search of academic literature through Google Scholar. I found several academic papers describing the results of crawling the Gnutella network. One in particular described developing a crawler that could access all the ultrapeers in the network in under 10 minutes in 2005. This work was titled "Capturing Accurate Snapshots of the Gnutella Network" by Daniel Stutzbach and Reza Rejaie, and appeared in 2005 at a prestigious peer-review networking conference.

93. A later publication using the same crawler also documented the files that were available on the Gnutella network. In this case, they modified the crawler above to also issue "browse host" requests to catalog the contents of the network. This work appeared in another prestigious

peer-reviewed conference in 2006 and was titled "Characterizing Files in the Modern Gnutella Network: A Measurement Study" by Shanyu Zhao, Daniel Stutzbach, and Reza Rejaie.

94. Looking at the authors list, it appears that Shanyu Zhao and Daniel Stutzbach were graduate students, and Reza Rejaie was a professor at the time. This small team, with no acknowledged funding, was able to develop a high-speed crawler that used the Gnutella browse host extension to catalog the network. This is one paper of many that describe crawling the Gnutella network.

95. I will also note that crawling Gnutella is a common enough activity that it has its own Wikipedia page at http://en.wikipedia.org/wiki/Gnutella_crawler.

96. This indicates that creating a crawler is not as difficult as Mr. Fisk implies, and certainly isn't the sole province of a large and well-funded organization.

ii. Crawling versus Sharing

97. In point g of his argument above, after suggesting the 1,718 File must have been found by a crawler from a large organization such as the FBI, Big Champagne, Tiversa, or the RIAA, Mr. Fisk then suggests that the other copies of the files that are available on the network might come from these crawlers.

98. Mr. Fisk is incorrect in this assertion because the organizations above, were they to download files, would have no motivation to then share them.

99. Instead, it is possible to download files without sharing them again on the network. Even an ordinary LimeWire user could prevent re-sharing files by separating the download folder from the shared folder.

E. Other Avenues of Information Disclosure

100. Complaint Counsel also asked me to provide an opinion about Mr. Fisk's conclusions as to other methods by which the 1,718 File could have been downloaded or disclosed. In this section, I discuss his conclusions about thumb drives and email.

101. After apparently reaching the erroneous conclusion that the installation and use of LimeWire could not have been a possible source of the 1,718 File leaving the LabMD network, Mr. Fisk attempts to propose some other mechanisms by which the file could have left the network. On page 25, he suggests that the file could have been emailed out of the organization or placed on a thumb drive and removed. Unfortunately, Mr. Fisk points to no evidence to support that either of these actions occurred. By contrast, there is ample evidence that LimeWire was in use.

102. One of my areas of research and experience is in the area of digital forensics, which is the investigation of misuse or crime that might have left evidence on digital devices. I have had extensive training in commercial forensics tools and operation and am well aware of the types of evidence that are left behind on a computer system when data is either copied to a USB stick or sent by email. It is frequently, though not always, possible to recover artifacts relating to these transfers. For a USB stick, there is evidence of what USB sticks were inserted into the system and, often, what files were copied to them. For email, it is often possible to recover the sent email from the outgoing messages folder or from backups from the mail server to verify what was sent.

103. Unfortunately, it is not possible to conduct such an examination in this case as the system that was being used was not properly preserved for investigation. Doing so would have required making a copy of the hard drive in its entirety and keeping the drive and copy unaltered. The

evidence is that this was not done.[27] As opposed to the lack of evidence for any of Mr. Fisk's alternate scenarios, there is substantial evidence that LimeWire was the source of the disclosure. We know that:

a. The computer at LabMD was running LimeWire and was sharing the 1,718 File.

b. People who download files from Gnutella most frequently store them in their own shared directory, which in turn makes them available to the file-sharing network.

c. The 1,718 File was found being shared on the Gnutella network. To appear there, it had to be placed in a folder on a computer that was being shared.

104. The most likely conclusion, then, is that the file was available and being shared via the LabMD computer. Others downloaded it, and as is common, stored it in their shared folder. It was then available for others to discover, and it was then found being shared elsewhere.

105. Overall, Mr. Fisk provides no evidence that supports his suggestion that the file was taken out of the network by some means other than through LimeWire.

VI. Conclusion

106. Based on my experience described in Section II, my review of the material described in Section IV, and the specific opinions presented in Section V, my overall conclusion is that Mr. Fisk is mistaken in his conclusion that the 1,718 File could only have been located by a sophisticated organization with considerable resources. In addition, his theory that the file was disclosed through a thumb drive or by e-mail is unsupported by any evidence. Overall, I conclude that the 1,718 File was likely inadvertently disclosed by LabMD's billing manager when she used LimeWire on her LabMD computer.

---

[27] Mr. Daugherty testified that the hard drive from the LabMD computer used by the billing manager and a copy of the hard drive were rendered unusable by a security consultant LabMD engaged. See Deposition of Michael Daugherty, March 4, 2014, pp. 203-07.

Dated: April 11, 2014

Clay Shields, Ph.D.

EXHIBIT 15

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of	)	
	)	
LabMD, Inc.,	)	Docket No. 9357
a corporation,	)	
Respondent.	)	

EXPERT REPORT OF RAQUEL HILL, PH.D.

TABLE OF CONTENTS

I. Introduction 1

II. Summary of Experience and Qualifications 2

III. Overview of Network Security Principles 4

- A. Background: Computer Networks 4
- B. Defense in Depth 8
- C. Principles for Assessing and Securing a Network 11

IV. LabMD's Network During the Relevant Time Period 13

V. Scope of Opinions 16

VI. Materials Considered in Forming Opinions 17

VII. Summary of Opinions 18

VIII. Opinions 19

- A. Comprehensive Information Security Program – Complaint ¶ 10(a) 19
- B. Risk Assessment – Complaint ¶ 10(b) 24
- C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c) 30
- D. Information Security Training – Complaint ¶10(d) 34
- E. Use of Authentication Related Security Measures – Complaint ¶10(e) 36
- F. Maintenance and Updating of Operating Systems– Complaint ¶10(f) 38
- G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g) 41

IX. Conclusion 46

EXPERT REPORT OF RAQUEL HILL, PH.D.

I. Introduction

1. I am a tenured professor of Computer Science at Indiana University with over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems.

2. The FTC has engaged me to testify as an expert in this litigation. As explained in more detail in Section V, below, Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information[1] within its computer network.

3. This report states my opinions and provides the justifications for those opinions. It also includes the following information:

- A summary of my experience and qualifications;
- An overview of network security principles and a description of LabMD's network; and
- A description of the materials that I considered in forming my opinions and conclusions.

4. Based on my review of the materials described in Section VI, below, and my experience described in Section II, below, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures. This conclusion covers the time period from January 2005 through July 2010

[1] For purposes of this report, Personal Information means individually identifiable information from or about an natural person including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. See Complaint Counsel's February 19, 2014 Requests for Admission to LabMD, p. 2.

(Relevant Time Period); as I explain in Paragraph 48, below, from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period. In section VIII, below, I present my specific opinions that support this conclusion.

II. Summary of Experience and Qualifications

5. I have over 25 years of combined academic, research, and industrial experience in computing. I received my B.S. degree with Honors in Computer Science from the Georgia Institute of Technology. As an undergraduate, I worked as a Cooperative Education student with IBM and received my Cooperative Education Certificate for working a minimum of six academic quarters with IBM as an undergraduate. This cooperative education experience allowed me to apply the theories that I was learning in the classroom, but also enabled me to help fund my degree.

6. I also received my M.S. degree in Computer Science from Georgia Tech. As an M.S. student, I worked for several companies, including: Cray Research, Hayes Microsystems, and Nortel Networks. My M.S. degree was funded by Cray Research via an academic scholarship.

7. After completing my M.S. degree, I worked for three years with Nortel Networks, where I designed and implemented network protocols that enabled telephone switches to communicate with remote devices. These protocols sustained communications even when a communications channel failed.

8. In 1996, I left Nortel Networks to pursue a Ph.D. in Computer Science at Harvard University. At Harvard, I designed and implemented a quality of service protocol that enabled routers in the network to reserve bandwidth for audio and video applications using a light-weight signaling protocol. As a part of this work, I evaluated the protocol to determine the threats and

vulnerabilities and designed mechanisms to secure the reservation process. I received my Ph.D. in October 2002, and began working as a lecturer within the School of Electrical Engineering at the Georgia Institute of Technology, where I taught a course in Digital Circuits. After working at Georgia Tech for 9 months, I accepted a position as a Post-Doctoral Research Associate with a joint appointment in the Computer Science Department and the National Center for Super Computer Application (NCSA) at the University of Illinois, Urbana-Champaign. As a Post-Doc, I designed and implemented mechanisms to secure environments where mobile devices and sensors are an integral part of the computing space. These spaces are often referred to as pervasive or ubiquitous computing environments. One of the major challenges to securing such environments is to apply uniform security policies across devices that have varying computational, space, and battery limitations.

9. After completing a two-year assignment at the University of Illinois, I joined Indiana University as an Assistant Professor of Computer Science in 2005. I was promoted to Associate Professor with tenure in 2012. Over the years, I have designed and taught classes in information and systems security including: Analytical Foundations of Security, Trusted Computing, Computer Networks, and Data Protection. My research areas span the areas of system security and data privacy. I have published articles on various topics, including: quality of service in networking, security for pervasive computing environments, encryption-based access control, reputation systems, trusted computing, smartphone security, and privacy in research datasets. I have published over 25 peer-reviewed articles and abstracts and given 25 invited technical talks and panels.

10. I am currently on sabbatical at Harvard University, where I am a Visiting Scholar within the Center for Research on Computation and Society at the School of Engineering and Applied Sciences. I am continuing my data protection research with a specific focus on medical data.

11. A more extensive summary of my professional accomplishments and a list of all publications that I have authored within the last 10 years can be found in my *curriculum vitae*, a copy of which is attached to this report as Appendix A. I have not testified as an expert at trial or at deposition within the last four years.

12. I am being compensated at a rate of $150 per hour for my work in connection with this litigation.

III. Overview of Network Security Principles

A. Background: Computer Networks

13. In this section, I describe very basic network functionality at a high level to support my opinions. A network is a collection of workstations, laptop computers, servers, and other devices (computers) that are connected via some communications channel that is either wired or wireless. In commercial settings, data is usually passed between computers within a network via a switch or a router. A switch and router can be combined into one device.

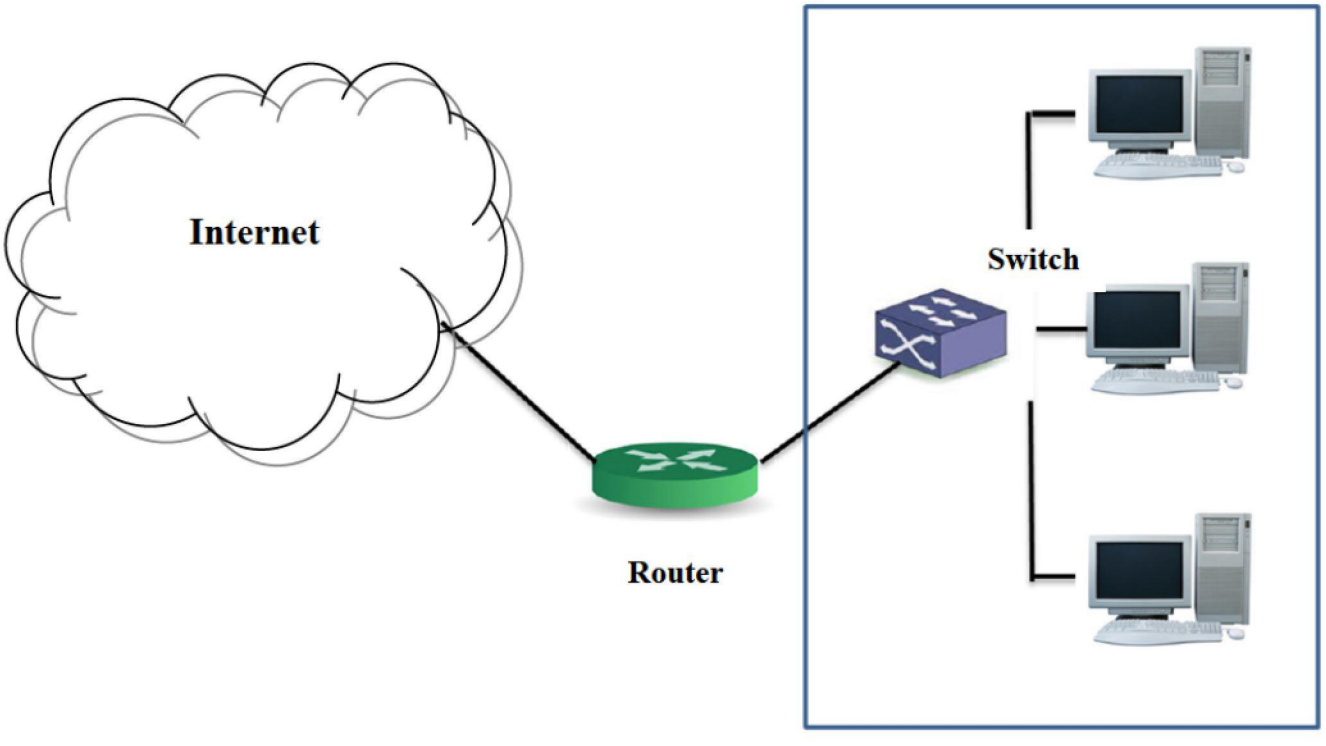
14. Computers use network interface cards (NIC) to connect to a network, and each NIC has a unique media access control (MAC) address. Each computer within a network is therefore uniquely identified by the MAC address of the computer's NIC. A computer's MAC address is not known outside of a computer's local area network (LAN).

15. A switch is a device that inspects incoming data to determine the destination MAC address and forwards the data to the computer with the specified MAC address.

16. A router is a device that connects networks. These networks may be of different types: wired vs. wireless, Ethernet vs. optical, etc. Routers forward data (in small units called packets) across the Internet using the Internet Protocol (IP) address of the destination computer. In doing so, the Domain Name System (DNS) is used to map a computer's hostname or a URL to an IP address. A computer's IP address is used by routers to forward data across the Internet to the specified destination network. Once the data reaches the destination network, the local switch uses the Address Resolution Protocol (ARP) to determine the MAC address of the computer that has the specified IP address. The switch passes the data to the destination computer.

17. **Figure 1** illustrates how a LAN may connect to the Internet. In the figure a switch connects the computers on the LAN and a router connects the LAN to the Internet. As noted in Paragraph 13, above, the function of the switch and the router can be combined into one device.

Figure 1: Connecting to the Internet



i. Network Addresses and Ports

18. In Paragraphs 13-16, I identified three types of addresses: Hostnames/URLs, IP addresses, and MAC addresses. DNS maps a hostname to an IP address, and ARP maps an IP address to a MAC address. The hostname and IP and MAC addresses are all needed to forward data to a specific computer. Once the data arrives at that computer, it must be sent to the application that is awaiting the information. The application is the ultimate recipient of any data that is sent to a computer on a network.

19. Applications are identified by numbers called ports. When data arrives at the destination, the receiving computer extracts the port number from the data and sends the data to the application that corresponds to that port number. Applications and their corresponding port numbers are the doors to computers and the networks to which the computers are connected. An application that contains a security vulnerability may allow an external entity to gain access to the LAN and any resources that are connected to the LAN. For this reason, it is important to ensure that all computers have been updated with all of the latest security patches for applications and related software

20. There are $2^{16} = 65{,}536$ possible ports on any computer. An open port is an open door to the computer, even when there is no application attached to the port. Therefore, it is important to close all unused ports on all computers. For example, when web access is not approved or authorized, ports 80 and 443 (which are typically used for web access) should be closed to prevent access to the computer through those ports.

ii. Firewalls and Intrusion Detection Systems

21. Firewalls are barrier mechanisms that are used to protect networks and individual computers. A firewall can be either a hardware device or a piece of software. It can be placed at a network gateway, or installed on a router or individual computer.

22. Firewalls can be configured to close all unused ports. When a port is closed, any data that arrives at the network or computer for that port will be discarded. Firewalls can also be configured to prevent and/or limit incoming connection requests. An incoming connection request is a request that originates from outside of the network but seeks to establish communication with a computer that is within the network. Only computers that are running authorized server applications should receive connection requests. A firewall, for example, could be configured to prevent all incoming connection requests for computers that are not running an authorized server application.

23. An intrusion detection system (IDS) is a device, typically another computer, that is placed inside a protected network to monitor activity in order to identify suspicious events. It can be either host-based or network-based. A host-based IDS runs on a single computer to protect that one host, while a network-based IDS is a stand-alone device that is attached to the network to monitor traffic throughout the network. An IDS acts as a sensor, like a smoke detector, that raises an alarm if specific things occur. It may perform a variety of functions including: monitoring users and system activity; auditing system configuration for vulnerabilities and misconfiguration; assessing the integrity of critical system and data files; identifying known attack patterns in system activity; recognizing abnormal activity through statistical analysis; managing audit trails and highlighting user violations of policy; correcting system configuration errors; and installing and operating traps to record information.

iii. Authentication and Access Control

24. Authentication and access control mechanisms prevent unauthorized access to computers, applications, services, and data.

25. To authenticate themselves, users provide a combination of information that tells the system who they are (identity) and information that proves that identity (proof). Usernames and passwords are commonly used to authenticate users. When authenticating, a user enters her username to identify herself to the authentication system, and her password to prove her identity. Some authentication mechanisms may require multiple forms of proof. For example, a user may be required to provide a password (what she knows), and proof of using something she possesses, such as a biometric (finger print, iris scan, etc.) or token. An authentication mechanism that requires two forms of proof is called two-factor authentication, and it is used as part of a defense in depth strategy (see Section III.B below) to reduce the risk of compromise. Remote login and access to highly sensitive data are scenarios for which either two-factor or multi-factor authentication is often used.

26. Access control mechanisms restrict a user's access to computers, services, applications, or data. An access control mechanism enforces policies that specify the resources that users may access. A user's role, security clearance, etc., may be used to identify the resources to which that user has access.

B. Defense in Depth

27. The most effective way to secure a network and its computers is by using multiple security measures to provide defense in depth. In such an approach, the network is viewed as a system with multiple layers, and security mechanisms are deployed at each layer to reduce the overall likelihood that an attack will succeed. The basic idea is not to rely on just one security

measure. Practicing defense in depth reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple defenses. To generally illustrate the benefit of defense in depth, assume that an attacker has a 50% chance of penetrating each defense mechanism. If there are three layers of protection, the probability of gaining unauthorized access to a resource at the innermost layer is $(1/2)^3 = 1/8$.

28. To illustrate the concept of network layers and defense in depth, consider Figure 1 above. In this simple network, the layers are: the router that connects the LAN to the Internet; the computers on the LAN; and applications on each computer on the LAN. Defense in depth on this network would require security policies and mechanisms to be specified and deployed at the router that connects the LAN to the Internet, at the workstations/servers, and at user accounts on those computers.

29. Continuing with the simple network in Figure 1, assume there is a risk that a company's employees will download and install on their computers applications they do not need to perform their jobs and that the company has a security policy prohibiting unauthorized applications. A simple prohibition that relies on employees following the policy does not provide defense in depth. A defense in depth strategy would prevent the employee from installing the application and/or limit the impact of an unauthorized application on the network. To achieve defense in depth, the company should use different security measures at different layers in the network, as follows:

a. **Internet Connection Layer:** At this layer, we cannot prevent software from being installed on a workstation or server, but we can restrict the type of traffic that flows into the network. Therefore, even if unauthorized software has been inadvertently installed on a workstation/server, mechanisms could be used to render the application

ineffective. Recall that port numbers map to specific applications, and that firewalls can be configured to restrict the types of application traffic that is allowed into the network, by dropping any data that contains an unauthorized port number. Thus, to illustrate the concept of defense in depth, a first line of defense to prevent use of unauthorized applications is to configure a firewall to close all ports at the gateway router except those that are used by authorized applications. Other mechanisms besides firewalls could be deployed at this layer as well, such as an IDS.[2]

b. **Workstation/Server Layer:** Even if a firewall were deployed at the gateway router, a second layer of security may be appropriate. The firewall at the gateway router may be misconfigured or not configured to discard all unauthorized traffic because the corresponding firewall policy would be hard to implement and manage. In these circumstances, a software firewall can be deployed at workstations and servers to further filter traffic that may have passed through the firewall at the gateway router. Because the firewall at a workstation or server is configured to protect that specific computer, the security settings can be more restrictive.

c. **User Account Layer:** Finally, in the simple network in Figure 1, user accounts for specific computers could be configured to so that system administrators can install software but ordinary users cannot.

30. As illustrated above, deploying security measures at different layers of a network enhances overall security by closing gaps in any one measure. In practice, achieving defense in

---

[2] A firewall and IDS could be used together to provide additional protection. If an IDS detects a violation, it could send a security alert to the system administration, indicating that unauthorized traffic is entering the network (i.e. traffic destined for an unauthorized application) and that firewall settings need to be updated to discard such traffic.

depth involves using layered security measures to address the many different risks and vulnerabilities a network may face.

C. Principles for Assessing and Securing a Network

31. There are seven principles that help to specify the policies and identify the mechanisms that are to be deployed at each layer of a defense in depth security strategy. These principles are listed and described below.

a. **Don't Keep What You Don't Need:** The first principle recognizes that maintaining sensitive information that is not needed creates an unnecessary risk.

b. **Patch:** A most basic principle is to Patch, meaning to apply updates to fix all known or reasonably foreseeable security vulnerabilities and flaws.

c. **Ports:** The third principle concerns Ports. As previously stated, applications communicate via ports. There are well-known ports for well-known applications. For example, a web server listens for incoming connections on Ports 80 and 443. All unused ports should be closed.

d. **Policies:** Policies are processes and procedures that are put in place to satisfy an organization's security requirements. Examples of policies would include the following:

- **Data Access** – Limit data access to persons with a need for the data.
- **Passwords** – Policies regarding passwords should contain rules about the following:
  - Acceptable minimum length.
  - Lifetime of a password.
    - The lifetime of a password is often related to the sensitivity of the information that the user accesses, the greater the sensitivity, the shorter the password's lifetime.
  - Password history.

- Passwords to avoid.
  - If you are a big sports fan, don't use a password that is related to your favorite team.
  - Avoid personal data such as spouse's name, children's name, pet's name, and birthdays.

- **Backups** – Backup data on a regular basis to be able to restore it because data is more valuable than the computer.
  - Encrypt backups.
  - Keep data in a secure location.
  - Limit access to backups.

e. **Protect:** Ensure that reasonable security software is employed, such as firewalls, anti-spyware, anti-virus, and IDS software, and authentication and access control. This list includes software that can be classified as either proactive or reactive. Proactive mechanisms attempt to prevent threats, while reactive mechanisms respond to threats that may have bypassed proactive mechanisms. Therefore, both types of mechanisms should be used to secure a system. Firewalls, authentication, and access control mechanisms try to block or prevent attacks. Anti-spyware, anti-virus, and IDS mechanisms attempt to detect the presence of malicious software or an attack while it is occurring.

f. **Probe:** Probing is a security audit that tests the state of a network. One type of probing is penetration testing, which searches the network for security flaws. Penetration testing includes scanning ports to verify that unused ports are closed or disabled. A thorough security probe would include a review of security policies, patching system, security logs, computers for unauthorized software, and any other processes, procedures, or information that may impact the security of a system.

g. **Physical:** There must be policies that govern the physical access to devices and data. Some examples of such policies include:

- Computer rooms must be locked.
- Server rooms must be locked with limited access.

IV. LabMD's Network During the Relevant Time Period

32. LabMD's network was small and simple. It included: computers LabMD provided to physician clients to use to place orders and retrieve results over the Internet; a small number of servers located at its business premises; and computers used by employees. In this section, I describe at a high level the network during the Relevant Time Period.

33. LabMD provided computers to physician clients. Through these computers, physician clients sent Personal Information over the Internet to LabMD. This information included names, addresses, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. In some instances, physician clients entered the information into the computer that LabMD had provided, one consumer at a time, and then sent the information to LabMD. In other instances, the LabMD computer in the physician's office retrieved Personal Information for all patients of the physician's practice from a database located on another computer in the physician's office and forwarded the information for all of those patients in bulk to LabMD, regardless whether LabMD performed testing for those patients.

34. The Personal Information LabMD received from physician clients typically was transmitted from physician clients to LabMD's network using a File Transfer Protocol (FTP) service LabMD installed on its network and the computers it provided to physician offices.

35. Regardless of whether Personal Information came as a bulk transfer or one consumer at a time, it was received by a server on LabMD's network (called Mapper), where it was processed (so that it could be used by applications LabMD used in is laboratory and billing department) and

then maintained on servers on the network. The laboratory and billing applications also ran on servers on LabMD's network. In addition, LabMD maintained Personal information on desktop computers, such as the Finance/Billing Manager's computer.

36. After LabMD's laboratory and medical employees had provided the services ordered by physician clients, they added results to the Personal Information LabMD maintained on its network.

37. The evidence in the record shows that LabMD did not encrypt Personal Information while it was maintained on LabMD's network.

38. Physician clients typically retrieved the results of the services they ordered from LabMD through LabMD's web portal. In doing so, they accessed Personal Information stored on LabMD's network.

39. LabMD's network included a number of servers that hosted applications, including back-up, email, webserver, database, laboratory, and billing applications. Some of these servers hosted multiple applications and also stored Personal Information. For example, one server hosted billing and mail applications[3]

40. Employees in the laboratory and billing departments, and certain other employees, used their LabMD computers to access resources on LabMD's network, including applications that provided access to Personal Information maintained on the network. Some LabMD employees could remotely access LabMD's network, including Personal Information maintained on the network.

---

[3] See, for example, FTC-LABMD-00002 (CX0034).

41. Record evidence shows that in 2005 or 2006, LimeWire, a peer-to-peer (P2P) file-sharing program, was installed on a computer on LabMD's network. The computer was used by the Billing Manager.

42. At a high level, the software is called peer-to-peer because users use it to search for and retrieve files directly from the computers of others using the software instead of retrieving files from a central server. To do this, the software allows users to designate or place files they will share in a folder (Sharing Folder). Using the software, a user can search the Sharing Folders of other users for files of interest. P2P programs have been widely available since 1999, and have been, and are, used by millions of users to share music, video, and other types of files.

43. Record evidence, including a screenshot of the Sharing Folder on the Billing Manager's computer taken in May 2008, shows that hundreds of files were in the Sharing Folder on the Billing Manager's computer.[4] Among these files was an insurance aging file (called the 1,718 File) that contained Personal Information about more than 9,300 people.[5] Copies of the 1,718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom.[6]

44. The risk of inadvertently sharing files with sensitive information using P2P software and the difficulty of undoing sharing are well known. After a file has been shared, the copy is out of the control of the original source and can be shared again from its new location to any number of other computers running the software. Searching for the file might not find all of the copies

---

[4] See FTC-LABMD-3755 (CX0152).

[5] See FTC-LABMD-3755 (CX0152); Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008)

[6] See Robert Boback, November 21, 2013 Deposition Transcript, pp. 50-53; TIVERSA-FTC_RESPONSE-000001 through TIVERSA-FTC_RESPONSE-006876 (CX0008-CX0011); TIVERSA-FTC_RESPONSE-006882 (CX0019).

because, for example, a computer with a copy might be turned off when the search occurs. Security professionals and others have warned about this risk since at least 2005.

V. Scope of Opinions

45. Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information within its computer network. Specifically, I was asked to analyze the record evidence relating to the following paragraphs of the FTC's complaint:

a. Paragraph 10: "At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

- (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;
- (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;
- (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- (d) did not adequately train employees to safeguard personal information;
- (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;
- (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely

that the systems would be updated to address newly discovered vulnerabilities; and

- (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks."

b. Paragraph 11: "Respondent could have corrected its security failures at relatively low cost using readily available security measures."

VI. Materials Considered in Forming Opinions

46. A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B. Those materials include: transcripts and exhibits from investigational hearings and depositions of LabMD, its current and former employees, and third parties; documents and correspondence provided to Complaint Counsel by LabMD and third parties in connection with the pre-complaint investigation or this litigation; and industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners. I also have relied upon my education and experience in reaching my opinions.

47. I am continuing to review material obtained by Complaint Counsel through discovery in this litigation. LabMD produced to Complaint Counsel more than 11,500 pages of documents between February 25 and March 4, 2014, and Complaint Counsel has informed me that depositions are noticed to be taken after March 18, 2014. I reserve the right to revise or supplement my opinions based upon my continued review of the documents recently produced by LabMD, information learned during depositions conducted after the submission of this report,

or any other new information relevant to this litigation that comes to my attention after the submission of this report.

48. As I noted in Paragraph 4, above, my overall conclusion and the specific opinions that support that conclusion cover the Relevant Time Period, which is January 2005 through July 2010. From my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.

VII. Summary of Opinions

49. Based on my review of the materials described in Section VI, above, and my experience described in Section II, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures. In reaching this conclusion, I have taken into account the amount and nature of the data maintained within LabMD's network, LabMD's network and security practices, risks and vulnerabilities on LabMD's network, and the cost of remediating those risks and vulnerabilities. Record evidence shows that LabMD maintains Personal Information about more than 750,000 consumers.[7] For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information.

50. In Section VIII, below, I present my specific opinions that support my overall conclusion. In each subpart of Section VIII, below, I present my specific opinions regarding whether LabMD

[7] See LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23. For most of those consumers, that information includes: Social Security numbers, insurance information, and medical diagnosis codes. See Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008).

could have corrected its security failings at relatively low cost using readily available security measures, which relate to Paragraph 11 of the Complaint.

VIII. Opinions

A. Comprehensive Information Security Program – Complaint ¶ 10(a)

51. Complaint Counsel has asked me to provide an opinion on whether LabMD developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information. My opinion is organized as follows: (1) an explanation of the contents of a comprehensive information security program; (2) my opinion, including some examples of key evidence supporting those opinions.

52. A comprehensive information security program is a plan that sets out an organization's security goals, the written policies that would satisfy those goals, the mechanisms that would be used to enforce the written policies, and how those mechanisms would be used to enforce the written policies. The best practices for developing a comprehensive information security program would include the seven principles that I discuss in Paragraph 31, above: don't keep what you don't need, patch, ports, policies, protect, probe and physical.

53. A comprehensive information security program should be in writing to provide guidance to those who are implementing the plan and those who receive training through the plan. It also should be in writing to record the organization's current security goals and practices to facilitate changes to those goals and practices as security threats continually evolve and, because turnover is inevitable, to communicate the security goals and practices of the organization to future employees.

54. An organization's comprehensive information security program should specify confidentiality, integrity, and availability goals, and related policies and mechanisms.

55. A confidentiality goal/policy ensures that only authorized individuals are able to access data. Encryption and access controls are mechanisms that can be used to enforce confidentiality policies. Encryption mechanisms are used to protect stored data and data that is being transmitted between parties, but encryption alone doesn't prevent unauthorized individuals from gaining access to the data. If I encrypt the data and distribute the encryption key to everyone, the encryption procedure is ineffective. Therefore, in addition to encrypting the data, an organization should specify under which conditions should data be accessed and which employees should be allowed to access the data. Role-based access control policies have been often used by organizations to differentiate the data access of employees. In such policies, employees are assigned data access rights based on the job that they are required to perform.

56. An integrity goal/policy ensures that data is not inadvertently changed or lost. Mechanisms that enforce an integrity policy ensure that any unauthorized changes to a system and its data can be detected. For example, cryptographic hash functions may be used to detect unauthorized changes to stored data (i.e. software executables, patient records) and transmitted data. A cryptographic hash function takes data input of any size and computes a fixed-size number called a hash value that is unique to the data and can be used as the digital fingerprint for the data. Thus, changes in a file's hash value indicates that the file has been changed. Integrity-based software scanners can be configured to detect newly added software and/or changes to existing application executables. Any new software that has been installed on a computer may indicate an unauthorized installation, while changes to existing executables may denote that malware has been embedded in an application.

57. An availability goal/policy specifies processes to ensure that the computing system (i.e. hardware, software, and network), and data are accessible, even in the presence of natural disasters or malicious attempts to compromise the system.

58. Achieving confidentiality, integrity, and availability goals may incorporate the use of a variety of security mechanisms, including firewalls, intrusion detection systems, integrity scanners, anti-virus scanners, backups, logging, authentication, physical security, access control, risk assessment, and remediation, etc.

59. While security goals, policies and mechanisms are key components of any security plan, the success of any defense-in-depth based information security program will be limited when the users and managers of the computing system are not properly trained. Therefore any comprehensive security plan should also include training procedures for non-IT and IT employees. This training should ensure that employees understand the security goals and policies and how to use any mechanisms that are to be used to secure the system. In addition, IT staff should receive training on specific mechanisms to mitigate risks and on evolving threats. I discuss the training component of a comprehensive information security program in more detail in Section VIII.D, below.

60. Securing electronic health data is a topic that has been explored by many national experts for years, which has resulted in the creation of best practices and guidelines for securing this information. Examples of comprehensive information security programs concerning electronic health data have been available online at no cost from various sources since as early as 1997, including, for example, the National Research Council (NRC), the National Institute of Standards and Technology (NIST), and the Health Insurance Portability and Accountability Act

(HIPAA) Security Rule.[8] These comprehensive security programs include guidelines for ensuring the confidentiality, integrity, and availability of data, including mechanisms for authenticating individual users, employing access control mechanisms to restrict access based on an individual's role, limiting a user's ability to install software, assessing risks and vulnerabilities, encrypting stored data and data in transit, logging access to data and system components, ensuring system and data integrity, protecting network gateways, maintaining up-to-date software, etc.

61. Based on my review of evidence from the record, I have formed the opinion that LabMD did not develop, implement or maintain a comprehensive information security program to protect consumers' Personal Information. Record evidence shows that:

a. From 2005 to 2010, LabMD had no written information security program.[9] During the Relevant Time Period, LabMD employees received an employee handbook, but this document did not address the practices covered by a comprehensive security program. For example, the handbook states that LabMD has taken specific measures to comply with HIPAA but does not explain those measures.[10]

---

[8] See, for example, National Research Council, For the Record: Protecting Electronic Health Information (1997), at http://www nap.edu/openbook.php?record_id=5595&page=R1; Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf; SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343; and Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[9] LabMD's Policy Manual, FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006) and LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual, FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007), were written in 2010. See, for example, John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 78-79, 91-92.

[10] See FTC-LABMD-003531 through FTC-LABMD-003553 (CX0001), p. 6; FTC-LABMD-003554 through FTC-LABMD-003575 (CX0002), p. 6.

b. Although LabMD contends that the policies set forth in LabMD's Policy Manual[11] were in place in 2007 and 2008, there is no documentation demonstrating that those policies were in place, and if they were in place, at least some of those policies were not being enforced. For example:

- LabMD contends that it adopted policies in 2002 to identify and remove unauthorized software that had been installed on employee computers and to configure firewalls on employee computers to block incoming connection requests. If these policies had been implemented, unauthorized software would have been detected and removed from employee computers, and computers located outside LabMD's network would not be able to initiate communications with computers inside the network. As discussed in Paragraphs 41-43, above, LimeWire, an unauthorized P2P file sharing program, was installed on the Billing Manager's computer in 2005 or 2006 and used to share files. LabMD's processes did not detect the software or prevent its use. LabMD removed the software in May, 2008, approximately two to three years from the date of installation, after being informed that the 1,718 File was found on a P2P network.

- In 2007 and 2008, when LabMD contends that the policies in its Policy Manual were in place, LabMD did not provide the encryption tools listed in its policy or provide staff with training on how to secure sensitive information included in emails or attachments.[12]

c. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual,[13] both of which were written in 2010, are not sufficiently comprehensive. For example, they lack specific policies that describe how Personal Information is protected during transmission between the physician offices and LabMD, and whether sensitive information is to be stored in an encrypted format.

---

[11] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 91-92.

[12] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 277-278; Alison Simmons May 2, 2013 Investigational Hearing Transcript, p. 163.

[13] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); FTC-LABMD-003590-3621 (CX0007).

- LabMD relied on the Secure Socket Layer (SSL) Protocol and HTTPS to encrypt communications and secure its web-based applications.[14] Record evidence shows that LabMD's servers allowed the use of SSL version 2.0, which had known security flaws.[15]

62. LabMD could have developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information at relatively low cost.[16]

B. Risk Assessment – Complaint ¶ 10(b)

63. Complaint Counsel has asked me to provide an opinion as to whether LabMD used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network, which is often called "risk assessment" in the IT field. My opinion is organized into several parts: (1) an explanation of why risk assessment is important; (2) a discussion of the mechanisms and protocols IT practitioners use to assess risks; and (3) my opinion, including some examples of key evidence supporting those opinions.

64. The relationship between risk assessments and reasonable security is very well known among IT practitioners, and frameworks for conducting risk assessments are widely available from many sources. When an assessment is inadequate or incomplete, network administrators and users may not know which risks or vulnerabilities they face and thus the security measures they should consider implementing. To IT practitioners, risk assessments are the foundation for choosing security measures that are reasonable and appropriate under their circumstances. It is an essential component of defense in depth.

65. IT practitioners use a variety of measures and techniques, to assess and remediate risks. These include antivirus applications, firewalls, various types of vulnerability scans, intrusion

---

[14] SSL is the protocol that ensures that data is encrypted for HTTPS.

[15] This vulnerability is discussed in Paragraph 100, below.

[16] See, for example, footnote 8, above, and the accompanying text.

detection systems, penetration tests, file integrity monitoring, and other measures. Typically, each mechanism can only assess the exposure to a particular type of risk or vulnerability. Antivirus applications, for example, can assess the incidence of viruses on a network, but not the installation of unauthorized applications on the network. Logs from firewalls, for example, can be reviewed to identify the application and host targets of unauthorized attempts to access the network, but traditional firewalls are designed to block specific types of traffic, not detect intrusions and attacks. An IDS can be used to detect attacks and alert the IT staff that firewall settings should be reconfigured. External vulnerability scans, which are conducted from outside the network, can, for example, assess the incidence of vulnerabilities in an application inside the network, but not the incidence of viruses. File integrity monitoring can identify changes in critical files that may indicate malware has been installed on the network, but does not identify or remove the malware. No one mechanism can assess the exposure to all the risks and vulnerabilities a network may face. An appropriate risk assessment process usually requires the use of a number of mechanisms.

66. Network administrators usually have a number of options to choose from in each mechanism category. For example, there are a number of branded antivirus applications, and within a brand there often are versions that differ in cost, the types of functions they can perform, and other aspects of performance. Properly used and reviewed, these mechanisms provide network administrators with essential information about risks and vulnerabilities they face. Having options provides companies with flexibility, so that they can balance the effectiveness of a mechanism, the sensitivity of the business and consumer information the assessment concerns, and the mechanism's cost.

67. Based on my review of the evidence from the record, I have formed the opinion that LabMD did not use an appropriate set of readily available measures to assess risks and vulnerabilities to the Personal Information within its computer network during the Relevant Time Period.

68. Record evidence shows that, prior to 2010, LabMD used antivirus applications, firewalls, and manual computer inspections to assess risks within the network. These mechanisms were not sufficient to identify or assess risks and vulnerabilities to the Personal Information maintained on LabMD's computer network.

a. As I discussed in Paragraph 65, above, antivirus applications can assess the incidences of viruses on a network but cannot assess the installation of unauthorized applications on the network. The evidence shows that at times, LabMD did not effectively manage its antivirus applications, or used applications that were out of date or had limited risk assessment functionality. For example, at some points, the antivirus application LabMD used on critical servers would not scan for viruses,[17] and thus could not identify risks to the servers. LabMD continued to use the same antivirus application after the vendor stopped providing updated virus definitions needed to identify newly discovered risks. On employee workstations, LabMD at times used antivirus applications that provided only limited risk assessment functionality, at least until late 2006. These applications could not be centrally managed by a network administrator; which meant that to be effective, individual employees had to update the virus definitions on their

[17] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

computers and report warnings to LabMD's IT Department. Even after it implemented a more capable antivirus application, LabMD did not install it on all its equipment.[18]

b. The firewall product that LabMD used until 2010 had very limited risk assessment capabilities. It could only log a few days of network traffic, which LabMD only reviewed to troubleshoot a performance problem, such as a user complaint that he or she could not connect to a website.[19] The firewall product also could not monitor traffic.[20] IT practitioners use traffic monitoring to, for example, determine if sensitive consumer information is being exported from their networks. LabMD could have used the freely available mechanism, Wireshark, to do packet level analysis to provide information to use to determine if Personal Information left the network without authorization.

c. Evidence in the record shows that, through at least mid-2008, LabMD conducted manual computer inspections only in response to a physician or employee reporting that a computer had malfunctioned.[21] Even when conducted on a regular basis, manual computer inspections can never be exhaustive because vulnerabilities and risks can exist anywhere in a computer, and human beings cannot inspect every one of those places. Even if they could, malicious software may, in some instances, mask its presence to avoid detection during a manual inspection, such as by altering the task manager application in Windows to prevent the malicious software's process from being displayed. For these reasons, IT practitioners should not rely on manual inspections and

---

[18] See, for example, Christopher Maire January 9, 2014 Deposition Transcript, p. 95; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 150-151.

[19] See, for example, Allen Truett February 27, 2014, Deposition Transcript, pp. 68-69.

[20] See, for example, Allen Truett February 27, 2014, Deposition Transcript, p. 67.

[21] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 177-178; Alison Simmons Investigational Hearing Transcript, pp. 78-80, 85-86; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 50-52.

should also use automated mechanisms, such as IDS, file integrity monitoring, and penetration testing to assess risks and vulnerabilities on the network.

69. LabMD did not implement an IDS or file integrity monitoring,[22] and only began conducting penetration tests in May 2010. These tests were limited to external facing servers and did not test employee workstations and computers inside LabMD's network. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using these automated mechanisms.

70. A penetration test of all IP addresses on the network, for example, would have identified vulnerabilities like outdated software, security patches that had not been applied, administrative accounts with default settings, etc. IT practitioners use this information to address these vulnerabilities. Information from penetration tests also could have identified all open ports within the network and all computers that accepted connection requests. This information could have been used to re-configure firewalls to close unneeded ports and to deny connection requests for computers whose work purpose didn't require the servicing of such requests.

71. Several well-respected and freely available penetration test and network analysis mechanisms have been available since 1997. Examples include: nmap (www.nmap.org, released 1997), Nessus (free until 2008), and Wireshark (formerly Etheral, released 1998). Using these mechanisms, LabMD could have conducted vulnerability scans, or had vulnerability scans conducted for it, throughout the Relevant Time Period, and doing so would have allowed it to correct significant risks, including those I describe in Paragraph 72, below, much sooner. The

---

[22] LabMD could have implemented an IDS and file integrity monitoring during the Relevant Time Period at relatively low cost. For example, LabMD could have implemented SNORT, a well-respected and widely used IDS that has been freely available since 1998, and, as I explain in Paragraph 104 below, Stealth and OSSEC are examples of freely available file integrity monitoring products.

cost of having penetration tests is modest: the penetration test LabMD had performed in 2010 by ProviDyn, an IT service provider, cost $450.[23]

72. Evidence in the record shows that the external vulnerability scans conducted in 2010 identified a number of well-known and significant risks and vulnerabilities on LabMD's network, including some that had been known to IT practitioners for years. For example, ProviDyn's April 2010 external vulnerability scan report identified a Level 5 anonymous FTP problem. This problem was first reported by the security community on July 14, 1993, 17 years before ProviDyn found it on LabMD's Mapper server.

73. Under the IT industry standardized classification system ProviDyn used, a Level 5 risk is an Urgent Risk and requires immediate remediation.[24]

74. The process for choosing reasonable and appropriate measures to address risks discovered through risk assessment is well-known and understood among IT practitioners and businesses. Guidelines on how to select reasonable and appropriate security measures have been freely available for years. NIST, for example, published a standard that explained the process in 2002.[25] In 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central

---

[23] See, for example, FTC-LABMD-003732 through FTC-LABMD-003736 (CX0044); FTC-LABMD-005254 through FTC-LABMD-005258.

[24] The risk classifications ProviDyn used are the classifications in the PCI Data Security Standard, which are derived from the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards (NIST). See PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1 (September 2006). In this classification, there are 5 levels: Urgent Risk (5), Critical Risk (4), High Risk (3), Medium Risk (2), and Low Risk (1). Level 5 (Urgent Risk) Vulnerabilities provide remote intruders with remote root/administrative capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers with full file-system read and write capabilities, remote execution of commands as an administrative user.

[25] See NIST Risk Management Guide for Information Technology Systems SP-800-30 (July 2002), at http://csrc nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

principles of NIST SP 800-30 in explaining how to perform the risk analysis and risk management required by the HIPAA Security Rule.[26]

75. IT practitioners have used these concepts to identify security measures that are reasonable and appropriate under various circumstances for years. The basic idea is to balance the severity of a risk and the harm that will result if the risk is exploited against the cost of a measure that remediates the risk. The more sensitive the Personal Information maintained within the network, the greater the need for enhanced security measures,

76. Consider the anonymous FTP problem set out in Paragraph 72, above: users are anonymous because no password is needed to log into the FTP service. It is an urgent risk to an application that LabMD used to transmit large amounts of Personal Information. Thus, the risk is high and the harm that would result if the risk were exploited is also high. The cost of remediating it is low, involving only IT-employee time to disallow anonymous log-ins. As a result, it would be reasonable and appropriate under these circumstances to disallow anonymous log-ins. The point of conducting appropriate risk assessments is to identify risks early, so that they can be remediated.

77. LabMD could have used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network at relatively low cost.[27]

C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c)

78. Complaint Counsel has asked me to provide opinions as to (1) whether LabMD maintained more Personal Information than necessary on its network and (2) whether LabMD

---

[26] See U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

[27] See, for example, Paragraph 71, above.

used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs. My opinion is organized as follows: (1) an explanation of why it is important for an organization to not maintain more Personal Information than necessary on its network; (2) my opinion concerning whether LabMD maintained more Personal Information than necessary on its network, including some examples of key evidence supporting those opinions; (3) an explanation of why limiting access to Personal Information is important; (4) a discussion of the mechanisms IT practitioners use to limit access to information maintained within a network; and (5) my opinion concerning whether LabMD used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs, including some of the evidence I considered.

i. Whether LabMD Maintained More Personal Information than Necessary

79. One of the principles of information security is for an organization to not maintain more information than it needs to conduct its business. This is important because, if an organization collects more data than is needed to conduct its business, it increases the scope of potential harm if the organization's network is compromised.

80. Based on my review of evidence from the record, I have formed the opinion that LabMD collected and maintained Personal Information about individuals for whom it has not performed testing (either directly or by outsourcing to another laboratory) and therefore did not use adequate measures to prevent employees from having access to Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD collected and maintained indefinitely Personal Information about approximately 100,000 consumers for whom it never performed testing (either directly or by outsourcing to another laboratory) and that

LabMD did not need to maintain Personal Information about those consumers in order to conduct its business.[28]

b. LabMD could have purged the data that it collected from consumers for whom it did not perform testing (either directly or by outsourcing to another laboratory) through its database applications. Purging data from a network is the type of thing that IT practitioners did regularly throughout the Relevant Time Period. Correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

ii. Whether LabMD Used Adequate Measures to Prevent Employees from Accessing Personal Information Not Needed to Perform Jobs

81. By not limiting access to data, an organization increases the likelihood that sensitive data will be exposed outside of the organization by either a malicious insider or a compromised system. Insider threat is one of the major issues facing organizations. Though some insiders do not have malicious intent, some scenarios create the perfect storm for the leaking of sensitive, personal data, especially health data. For example, in recent years, there have been several highly publicized events where individuals with celebrity status had their personal health information exposed by an insider of the health care organization. While these events are publicized, there are numerous others that are not. Friends, family members, co-workers or acquaintances access the personal health records of an individual outside of the organizations' policy, thereby violating that individual's right to privacy. To address this problem an organization must specify policies and employ mechanisms that limit an employee's access to data based on that which is needed to perform their daily tasks. For example, a lab tech may need information that identifies

---

[28] LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23; Michael Daugherty March 4, 2014 Deposition Transcript, pp. 198-199.

the patient, but may not need the patient's insurance information. Additionally, when an organization has information about a large number of people, it is not only necessary to limit the types of information that an employee within a specific role may access, but it is also important to limit the number individuals whose Personal Information the employee may access. Doing so reduces the impact of a malicious insider.

82. In addition to the insider threat, when data may be accessed by multiple parties, the likelihood that the data may be accessed from a computer that has been compromised also increases. This is especially the case for organizations that do not have a comprehensive information security plan, and have security practices that are at best reactive. In such cases, when data is downloaded to a compromised computer, vulnerabilities on that computer may expose the data to individuals outside of the organization.

83. A multi-pronged, defense in depth, approach must be used to effectively restrict access to data. The organization must first define roles for its employees and specify the types of data that are needed to complete the tasks that have been assigned to those roles. To enforce these roles, IT practitioners have long used role-based access control mechanisms to restrict access to sensitive data resources. These mechanisms should be employed to restrict access to data files and to applications that mediate access to the data.

84. Based on my review of evidence from the record, I have formed the opinion that LabMD did not use adequate measures to prevent employees from accessing Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD is unable to specify the types of Personal Information that each of its employees was permitted to access via LabMD's network and can specify only that its employees had "various levels of access" to various types of

Personal Information and that "all employees could gain knowledge of any Personal Information regarding Consumers to the extent it was necessary to the performance of their job duties."[29]

b. Because LabMD cannot specify the types of Personal Information that each of its employees was permitted to access via LabMD's network, I conclude that LabMD did not specify policies and employ mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs.

85. LabMD could have specified policies and implemented access control mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs at relatively low cost. Operating systems and applications have access control mechanisms embedded in them. Therefore, correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

D. Information Security Training – Complaint ¶10(d)

86. Complaint Counsel has asked me to provide an opinion as to whether LabMD adequately trained employees to safeguard Personal Information. My opinion is organized as follows: (1) an explanation of the importance of training; and (2) my opinion, including some examples of key evidence supporting those opinions.

87. The user is the weakest link in any information security program. A flawless security mechanism can be rendered ineffective by an untrained user. For example, a username/password

---

[29] LabMD's February 20, 2014 and March 17, 2014 responses to Complaint Counsel's Interrogatory No. 2. See also, for example, March 10, 2014 Order on Complaint Counsel's Motion for Discovery Sanctions, p. 5.

authentication mechanism is only effective when users create strong passwords. Weak passwords that are short in length, contain dictionary words, contain the names of relatives, or favorite sports teams are more easily guessed than others. Therefore, an organization should train its employees on how to use any security mechanisms that require employee action or any security mechanisms that employees are not technically prevented from reconfiguring (such as disabling a firewall on a workstation without IT staff approval).

88. Employees also should receive periodic training on expected and acceptable use of computing facilities and current threats and best usage practices.

89. Since computer threats and vulnerabilities are always evolving, IT practitioners should receive periodic training on the most recent advances in protecting against such threats. Several nationally recognized organizations provide low-cost and free IT security training courses.[30]

90. I see no evidence in the record indicating that LabMD's non-IT employees received training on how to use security mechanisms or training on the consequences of reconfiguring security settings in applications and security mechanisms on their computers, such as enabling file-sharing, which I discuss in Section VIII.G, below.

91. Record evidence shows that LabMD did not adequately train employees to safeguard Personal Information or provide appropriate opportunities for its IT employees to receive formalized security related training about evolving threats and how to protect against them.[31] This resulted in gaps in their knowledge and a creation of security processes that were reactive, incomplete, ad hoc, and ineffective. For example, prior to 2010:

---

[30] For example, the Center for Information Security Awareness, formed in 2007, provides free security training for individuals and businesses with less than 25 employees. The SysAdmin Audit Network Security Institute (SANS) formed in 1989, provides free security training webcasts. Additional free training resources may be found at http://msisac.cisecurity.org/resources/videos/free-training.cfm. The Computer Emergency Response Team (CERT) at Carnegie Mellon University has e-learning courses for IT professionals for as low as $850.

[31] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 52-53, 60-61.

a. Penetration testing was never done;[32]

b. Software with known flaws was not updated on servers that contained Personal Information;[33]

c. Firewalls were disabled on servers that contained Personal Information;[34]

d. Servers executed software that was no longer supported by vendors, including operating system and antivirus software;[35]

e. There was no uniform policy requiring strong passwords or expiration of passwords;[36]

f. Personal Information was transmitted and stored in an unencrypted format;[37]

g. At least some employees were given administrative access accounts and were able to download and install software without restriction, etc.[38]

92. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost.[39]

E. Use of Authentication Related Security Measures – Complaint ¶10(e)

93. Complaint Counsel has asked me to provide an opinion as to whether LabMD required employees, or other users with remote access to the network, to use common authentication-

---

[32] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 92, 281-282.

[33] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[34] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 293-294.

[35] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274; FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

[36] See, for example, Robert Hyer December 13, 2013 Deposition Transcript, pp. 25-27, 45-46; Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 153-154; John Boyle February 5, 2013 Investigational Hearing Transcript, pp. 181-184.

[37] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 62-64, 302-304.

[38] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 172; Alison Simmons Investigational Hearing Transcript, pp. 37-39; Robert Hyer December 13, 2013 Deposition Transcript, pp. 27-29.

[39] See, for example, footnote 30, above, and the accompanying text.

related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication. My opinion is organized as follows: (1) an explanation of why using authentication-related security measures is important; (2) a discussion of common authentication-related security measures to limit access; and (3) my opinion, including some examples of key evidence supporting those opinions.

94. Organizations should use strong authentication mechanisms to control access to workstations. Usernames/passwords are one such mechanism, but the effectiveness of this mechanism depends on the strength of the passwords and how the passwords are stored and managed. An organization should specify policies on how to create strong passwords. For example, password policies should specify acceptable length, required characters (numbers, case, symbols), lifetime, password history, passwords to avoid, etc. To enforce these policies: password management should be centralized; passwords should not be stored in clear text; and a cryptographic hash should be applied to the password before it is stored.

95. Based on my review of evidence from the record, I have formed the opinion that LabMD did not require employees or other users with remote access to its network, to use common, effective authentication-related security measures.

a. Record evidence shows that LabMD did not provide specific strong password policies or enforcement mechanisms to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network, either on site or remotely. For example:

- LabMD billing employee Sandra Brown testified that she used the same username, sbrown, and password, labmd, to access her LabMD computer on site and remotely from 2006 to 2013.[40]

---

[40] See Sandra Brown January 11, 2014 Deposition Transcript, p. 13.

- LabMD created weak passwords for the nurses' user accounts that were created on the computers that it placed in its physician clients' offices. The typical password included the nurse's initials.[41]

- Although the Windows operating systems that LabMD used provided a centralized scheme to manage passwords, LabMD did not use that functionality.[42]

- Requiring two-factor authentication for remote users would have implemented a defense in depth strategy and could have compensated for LabMD's failure to require the use of strong passwords. LabMD did not use two-factor authentication.[43]

b. Record evidence shows that between at least October 2006 and June 2009, passwords required for access to Personal Information were shared by multiple LabMD employees.[44]

96. LabMD could have easily implemented strong authentication-related security measures at low cost.

F. Maintenance and Updating of Operating Systems– Complaint ¶10(f)

97. Complaint Counsel has asked me to provide an opinion as to whether LabMD maintained and updated operating systems of computers and other devices on its network. My opinion is organized as follows: (1) an explanation of the risks of using outdated software; and (2) my opinion, including some examples of key evidence supporting those opinions.

---

[41] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 46-48; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 39-41.

[42] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 171-172; Robert Hyer December 13, 2013 Deposition Transcript, pp. 84-88.

[43] See, for example, Alison Simmons, May 2, 2013 Investigational Hearing Transcript, pp. 47, 144, 152, 156; Curt Kaloustian May 3, 2013, Investigational Hearing Transcript, pp. 254-258; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 83-84; Lawrence Hudson January 13, 2014 Deposition Transcript, pp. 74-75, 89, 183; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 38-41.

[44] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 79; Robert Hyer December 13, 2013 Deposition Transcript, pp. 26-27, 45, 62, 74-75.

98. Researchers have found that experienced programmers introduce 1 bug per every 10 lines of code that they write.[45] Therefore, for a program like Windows Server 2003[46] that has 50 million lines of code, you can expect approximately 5 million software bugs to be introduced while the software is being developed. While many of the bugs will be detected and fixed during system testing, not all bugs will be identified before the product is shipped. In addition, code that was added to fix a problem may also introduce new bugs.

99. Hackers exploit software bugs to gain unauthorized access to computer resources and data. To limit these exploits, IT practitioners should connect to product notification systems and immediately apply remediation processes and updates for vulnerabilities that have been identified. These systems provided freely available notifications from vendors, CERT, OSVDB, NIST, and others throughout the Relevant Time Period.

100. Based on my review of evidence from the record, I have formed the opinion that through at least 2010, LabMD did not adequately maintain and update operating systems of computers and other devices on its network.

a. Record evidence shows that LabMD servers executed software that had vulnerabilities that had been identified and reported by the security and IT community several years prior to being detected on LabMD computers.[47] This time delay indicates that LabMD was neither knowledgeable of nor responsive to security alerts and software updates for the products that it used.

---

[45] See Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional 1995.

[46] LabMD used Windows Server 2003 on at least some of its servers in May 2010. See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[47] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

b. Record evidence shows that LabMD did not apply software updates in accordance with the policies it claims were in place during the Relevant Time Period[48] and had no policy for updating the software on hardware devices such as firewalls and routers.

c. Record evidence shows that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft.[49] The support life-cycle for Windows NT 4.0 ended on June 30, 2004, and Microsoft retired public and technical support and security updates on December 31, 2004. In a Microsoft press release, Microsoft states "Microsoft is retiring support for these products because the technology is outdated and can expose customers to security risks. The company recommends that customers who are still running Windows NT 4.0 begin migrations to newer, more secure Microsoft operating system products as soon as possible."[50]

d. Record evidence shoes that the LabMD Labnet server was running a version of Veritas Backup software that was configured with the default administrative password. This vulnerability had a Level 5 (Urgent Risk) rating, which means that an attacker can compromise the entire host. This problem was detected in 2010, and the corresponding solution was available as early as August 15, 2005. The Veritas software on the Labnet server also contained a Level 4 (Critical) buffer overflow vulnerability that would allow an attacker to execute arbitrary code on the remote host.[51] This problem was also detected

---

[48] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035); FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006); FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007).

[49] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274.

[50] "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.

[51] Level 4 risks are "Vulnerabilities expose highly sensitive information and provide hackers with remote user capabilities. Intruders have partial access to file system; for example, full read access without full write access."

in 2010, and the corresponding solution was made available by the vendor on July 11, 2007.

e. Record evidence shows that several LabMD servers were running Integrated Information Services (IIS) web servers that used an insecure version of the Secure Socket Layer protocol (SSL 2.0).[52] This vulnerability had a Level 3 (High Risk) rating, which means that it provided hackers with access to specific information on the host, including security settings.[53] The vulnerability was detected on LabMD servers in 2010. Microsoft provided instructions on how to disable SSL 2.0 as early as April 23, 2007. Microsoft released Windows Server 2008 along with IIS 7.0 on February 27, 2008 and recommended both as upgrades to address the SSL 2.0 flaw. Thus, remediation for the flaw was available for three years prior to the vulnerability being detected on LabMD's network by the ProviDyn scan.

101. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost.

G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g)

102. Complaint Counsel has asked me to provide an opinion as to whether LabMD employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. My opinion is organized as follows: (1) an explanation of the available measures and how they could have been deployed to prevent or detect unauthorized access to

---

[52] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070). SSL is the protocol that ensures that data is encrypted for https.

[53] Level 3 risks are "High Risk vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying)." FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

Personal Information; and (2) my opinion, including some examples of key evidence supporting those opinions.

103. Since security threats and vulnerabilities are changing constantly, security mechanisms that prevent an attack can never be exhaustive. Therefore, a defense in depth strategy must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker and detect unauthorized access when an attack is successful. The process of detection enables the organization to identify and patch holes in its security system.

104. There are several proactive, measures that should be employed, as part of a defense in depth strategy, to prevent the unauthorized sharing of Personal Information with external entities, including:

a. Employees should be given non-administrative accounts on workstations, thereby preventing them from installing software. Windows includes the functionality to enforce this policy in its operating systems package. This is a cost free measure.

b. Backups of Personal Information should be stored on devices that are isolated from other employee activities. An employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, etc. Therefore, backups of Personal Information should not be stored on multi-purpose employee workstations. Enforcing such a policy could be cost-free, if the organization designated an existing device for storage purposes only.

c. Windows operating systems provide the functionality to allow users to create folders that are stored on their individual workstations that can be shared with others.[54]

---

[54] These folders are different from shared folders on a network server that are centrally managed by IT staff.

When a folder is shared, it allows others to view the files that are contained within the folder.

d. While shared folders facilitate document sharing within an organization, there are many opportunities to mis-configure the sharing settings, which may lead to the inadvertent sharing of sensitive information with unauthorized parties. Such misconfigurations may include: giving read/write permissions to unauthorized parties, including restricted files in the shared folders, not including password protection, etc. In addition to the risk of misconfigurations, file-sharing applications, like LimeWire, also present the contents of shared folders to other users of those applications as information that is available to be downloaded. Therefore, employees should not be permitted to create shared folders on their workstations. Enforcing a no-shared folders policy requires no additional software, and can be achieved by configuring folder settings to disallow sharing and periodic monitoring of those settings.

e. A firewall should be employed at the network gateway to block all unwanted traffic from entering the network. The gateway firewall could be configured to block traffic destined to all unauthorized applications, such as file-sharing applications, which in turn would prevent traffic for those applications from entering the network. This type of configuring would create a list of acceptable applications and was routinely done by IT practitioners throughout the Relevant Time Period.

f. In addition, all employee workstations should be configured to use a software firewall. On August 25, 2004, Microsoft released its Windows Firewall as part of Windows XP Service Pack 2. This software firewall could be configured to block all incoming connection requests to a workstation. This would prevent, for example, users of

file-sharing applications, like LimeWire, from establishing a successful connection with a workstation and downloading shared files. The Windows Firewall accompanied the operating system at no cost to the customer.

g. Properly configuring firewalls at the network gateway and on employee workstations implements a defense in depth strategy for network protection. This provides protection and the outer network layer and the inner workstation layer to provide more robust protection against unauthorized attempts to access the network infrastructure.

h. File Integrity Monitors (FIM) take an initial snapshot of the files that are stored on a computer and periodically monitor the system to determine whether any changes have occurred. Any change may indicate malicious activity and raises an alert notification, indicating further investigation is needed. A FIM can be used to determine the presence of unauthorized software on a system. There are both free and commercially available FIM products. Stealth[55] and OSSEC are examples of free products, and Tripwire is an example of a commercial product. These are the types of mechanisms that IT practitioners used regularly throughout the Relevant Time Period.

105. Based on my review of evidence from the record, I have formed the opinion that LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network.

a. Record evidence shows that LabMD actively stored backups of highly sensitive Personal Information on the Billing Manager's workstation.[56] At least one document

---

[55] "Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host," http://stealth.sourceforge.net/, accessed on March 17, 2014.

[56] See FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006).

containing [a backup of] Personal Information was stored in a shared folder on the Billing Manager's workstation, which made it accessible to the unauthorized file-sharing application that had been previously installed on that computer.

b. As discussed in Paragraph 61, above, record evidence shows that LabMD did not detect and remove the file-sharing application, LimeWire, until 2008, two to three years after it had been installed.[57] Had LabMD used FIM products to periodically monitor the Billing Manager workstation during this two to three year period, it might have detected the LimeWire application by, for example, detecting its installation or detecting music files downloaded through LimeWire. FIM therefore would have strengthened a defense in depth approach.

c. Record evidence shows that LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network.[58]

106. LabMD could have employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network at relatively low cost.

---

[57] See, for example, July 16, 2010 Letter from P. Ellis to A. Sheer (FTC-LABMD-002495 through FTC-LABMD-002503).

[58] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 98-103.

IX. Conclusion

107. Based on my review of the materials described in Section VI, above, my experience described in Section II, above, and the specific opinions presented in Section VIII, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network throughout the Relevant Time Period of January 2005 through July 2010, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures.

Dated: March 18, 2014

Raquel Hill, Ph.D.

Appendix A

Home Address:
734 E. Moss Creek Drive
Bloomington, IN 47401
Phone(217)369-0105
hill raquel@gmail.com

School of Informatics and Computing
Indiana University
Bloomington, IN 47405
Phone (812) 856-5807
E-mail
ralhill@indiana.edu
www.cs.indiana.edu/~ralhill

Raquel Hill

Education

University of Illinois Urbana, IL
August 2003- July 2005 Post Doctoral Research Associate

Harvard University Cambridge, MA
November 2002 PhD Computer Science

- Dissertation: Sticky QoS: A Scalable Framework for Resource Reservations.
- Advisor: H.T. Kung

Georgia Institute of Technology Atlanta, GA
March 1993 MS Computer Science
June 1991 BS Computer Science with Honors

Professional Experience

Harvard University, Cambridge, MA, **Visiting Scholar,** School of Engineering and Applied Science, **Center for Research on Computation and Society,** 9/2013 – 5/2014

Indiana University, Bloomington, Indiana, **Associate Professor,** School of Informatics and Computing, 6/2012 –Present

Indiana University, Bloomington, Indiana, **Assistant Professor,** School of Informatics and Computing, 08-2005 – 6/2012

Indiana University, Bloomington, Indiana, **Research Fellow**, **Kinsey Institute**, 12/2010 – Present

Jackson State University, Jackson, Mississippi, **Adjunct Professor, Department of Computer Science**, 2010- Present

University of Illinois, Urbana, Illinois, **Post-Doctoral Research Associate,** Joint Appointment with Department of Computer Science and NCSA, 08/2003 – 07/2005

Georgia Institute of Technology Atlanta, GA, **Lecturer,** within the School Electrical and Computer Engineering, 11/2002 – 08/2003

Professional Experience

Harvard University, Cambridge, MA, **Research Assistant** 09/1998 – 09/2002

IBM Research , Hawthorne, NY**, Intern**, Summer 1999

Digital Equipment Corporation, Cambridge, MA, **Intern**, Summer 1997

Nortel Networks , RTP, NC, **Member of Scientific Staff**, 08/1993 – 08/1996

Hayes MicroComputer Products, Atlanta, GA, **Coop Student**, 03/1993-07/1993

Cray Research, Eagan, MA, **Intern**, Summer 1992

Cray Research, Chippewa Falls, WI, **Intern,** Summer 1991

IBM Corporation, Atlanta, GA, **Co-op Student**, 06/1987-9/1990

Grants

IBM Corporation, Equipment Grant – Cryptographic Co-processors
Equipment Value: $75,000.00 Date: 9/01/05 – Present

CACR: Privacy Enhanced Online Human Subjects Data Collection
Total Award Amount: $49,999.99 Date: 07/01/09 – 12/31/10
Role: PI Source of Support: IU

TC: Large: Collaborative Research: Anonymizing Textual Data and Its Impact on Utility
Total Award: $568,895 Date: 9/01/10 – 8/31/14
Role: PI Source of Support: NSF

FRSP: Childhood Obesity Studies with Secure Cloud Computing
Total Award: $36,500 Date: 9/1/11 – 12/31/13
Role: PI

Publications

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J. R. Heiman, L. Xiong, Evaluating Utility: Towards an Understanding of Sharing Differentially Private Behavioral Science Data, (Under Review).

Raquel Hill, Michael Hansen, Veer Singh, "Quantifying and Classifying Covert Channels on Android", *Journal of Mobile Networks and Applications*, Springer US. DOI. 10.1007/s11036-013-0482-7, (November 2013).

Publications

D. Hassan, R. Hill, "A Language-based Security Approach for Securing Map-Reduce Computations in the Cloud", To appear in the *Proceedings of the 6th IEEE/ACM International Conference on Utility and Cloud Computing*, December 9-12, 2013, Dresden, Germany.

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J.R. Heiman, L. Xiong, "An Empirical Analysis of a Differentially Private Social Science Dataset" In the *Proceedings of PETools: Workshop on Privacy Enhancing Tools, Held in Conjunction with the Privacy Enhancing Tools Symposium*, July 9, 2013, Bloomington, IN.

M. Hansen, R. Hill, S. Wimberly, Detecting Covert Communications on Android. In the *Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN 2012)*, October 22-25, 2012, Clearwater, Florida.

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, J. Heiman, Uniqueness and How it Impacts Privacy in Health-Related Social Science Datasets, In the Proceedings of the *ACM International Health Informatics Symposium (IHI 2012)*, January 28-30, 2012, Miami Florida.

J. Harris, R. Hill, Static Trust: A Practical Framework for Trusted Networked Devices, In the *Proceedings of 44th Hawaii International Conference on System Sciences, Information Security and Cyber Crime Track*, (Kauai, HI, 2011), 10 pages, CDROM, IEEE Computer Society.

Al-Muhtadi, Raquel Hill and Sumayah AlRwais "Access Control using Threshold Cryptography for Ubiquitous Computing Environments". *Journal of King Saud University Computer and Information Sciences*, No. 2, Vol. 23, (July 2011).

R. Hill, J. Al-Muhtadi, W. Byrd, An Access Control Architecture for Distributing Trust in Pervasive Computing Environments, at the *6th IEEE/IFIP Symposium on Trusted Computing and Communications (TrustCom)*, In the *Proceedings of 8th IEEE/IFIP Conference on Embedded and Ubiquitous Computing*, (Hong Kong, China, 2010), 695-702.

J. Harris, R. Hill, Building a Trusted Image for Embedded Communications Systems, In the *Proceedings of 6th Annual Cyber Security and Information Intelligence Workshop*, (Oakridge, TN, 2010), ACM, NY, 65:4.

L. Wang, R. Hill, Trust Model for Open Resource Control Architecture, at *3rd IEEE International Symposium on Trust, Security and Privacy for Emerging Applications*, In the *Proceedings of 10th IEEE International Conference on Computer and Information Technology*, (Bradford, UK, 2010) 817-823.

Publications

Gilbert, J.E., MacDonald, J., Hill, R., Sanders, D., Mkpong-Ruffin, I., Cross, E.V., Rouse, K., McClendon, J., & Rogers, G. (2009) Prime III: Defense-in-Depth Approach to Electronic Voting. In the *Journal of Information Security and Privacy*, 2009

J. Al-Muhtadi, R. Hill, R. Campbell, D. Mickunas, Context and Location-Aware Encryption for Pervasive Computing Environments, In *Proceedings of the 4th IEEE Conference on Security in Pervasive Computing and Communications Workshops*, (Pisa, Italy, 2006), 283-289.

R. Hill, S. Myagmar, R. Campbell, Threat Analysis of GNU Software Radio, In the *Proceedings of the 6th World Wireless Congress*, (San Francisco, CA, 2005).

A. Lee, J. Boyer, C. Drexelius, P. Naldurg, R. Hill, R. Campbell, Supporting Dynamically Changing Authorizations in Pervasive Communication Systems, In the *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, (Boppard, Germany, 2005), 134-150.

R. Hill, G. Sampemane, A. Ranganathan, R. Campbell, Towards a Framework for Automatically Satisfying Security Requirements, In the *Proceedings of Workshop on Specification and Automated Processing of Security Requirements in conjunction with the 19th IEEE International Conference on Automated Software Engineering*, (Linz Austria, 2004), 179-191.

R. Hill, J. Al-Muhtadi, R. Campbell, A. Kapadia, P. Naldurg, A. Ranganathan, A Middleware Architecture for Securing Ubiquitous Computing Cyber Infrastructures, *5th ACM/IFIP/USENIX International Middleware Conference,* October 2004, *in IEEE Distributed Systems Online*, 5,9 (September 2004), 1-.

R. Hill, H.T. Kung, A Diff-Serv enhanced Admission Control Scheme, In *Proceedings IEEE Global Telecommunications Conference,* (San Antonio, TX, 2001), 2549-2555.

Refereed Abstracts

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, Privacy and De-Identification in High Dimensional Social Science Data Sets, *in the Proceedings of the 32nd Annual IEEE Symposium on Security and Privacy* , Oakland, California, May 22-25, 2011.

R. Hill, J. Camp, Communicating Risk within the GENI Infrastructure, *Workshop on GENI and Security,* University California, Davis, January 22-23, 2009.

R. Hill, J. Wang, K. Nahrstedt, Towards a Framework for Quantifying Non-Functional Requirements, *Grace Hopper Celebration of Women in Computing*, October 2004.

Refereed Abstracts

J. Al-Muhtadi, R. Hill, R. Campbell, A Privacy Preserving Overlay for Active Spaces, *Ubicomp Privacy Workshop in conjunction with the Sixth International Conference on Ubiquitous Computing*, Nottingham, England, September 2004.

Posters

R. Hill, A.C. Solomon, E. Janssen, S. Sanders, J. Heiman, Privacy and Uniqueness in High Dimensional Social Science and Sex Research Datasets, Presented at the 37th Annual Meeting of the International Academy of Sex Research, August 10-13, 2011, Los Angeles, California.

C. Boston, R. Hill, L. Moore, The Feasibility of Designing a Secure System to Prevent Surgical Errors Using RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

S. Camara, R. Hill, L. Moore, Understanding How RFID Technology Impacts Patient Privacy, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Johnson, R. Hill, L. Moore, Evaluating and Mitigating the Security Vulnerabilities of RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Hill, J. Wang, K. Nahrstedt, Quantifying Non-Functional Requirements: A Process Oriented Approach, *in the Proceedings of the 12th IEEE International Requirements Engineering Conference,* Kyoto, Japan, September 2004.

Technical Reports

R. Hill, J. Al-Muhtadi, Building a Trusted Location Service for Pervasive Computing Environments, Technical Report, TR646, Computer Science, Indiana University, 2007.

Dissertation

R. Hill, Sticky QoS: A Scalable Framework for Resource Reservations, Doctoral Dissertation in Computer Science, Harvard University Division of Engineering and Applied Sciences, November 2002.

Symposiums

"Protecting Privacy in Sex Research: Challenges and solutions offered by new technologies and recommendations for the collection, protection and the sharing of multi-dimensional data", **Speakers:** Raquel Hill, School of Informatics and Computing, Indiana University, Ulf-Dietrich Reips, iScience, University of Deusto, Bilbao, Spain, Stephanie Sanders, Gender Studies, Indiana University, The 38th Annual Meeting of the International Academy of Sex Research, July 8-12, 2012, Lisbon, Portugal

Invited Talks

"Understanding the Risk of Re-Identification in Behavioral Science Data", Technology in Government Topics in Privacy Seminar, Data Privacy Lab, Harvard University, Cambridge, MA, November 4, 2013.
.

Invited Talks

"Evaluating the Utility of a Differentially Private Behavioral Science Dataset", Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, MA, October 2, 2013.

"Balancing the Interests in Developing and Sharing Behavioral Science Data", Workshop on Integrating Approaches to Privacy Across the Research Lifecycle, Harvard University, Cambridge, MA, September 24-25, 2013.

"Kinsey Goes Digital", Kinsey Institute's Board of Trustees Meeting, Indiana University, Bloomington, IN, May 20, 2011.

"Integrity-Based Trust for Networked Communications Systems", Center for Applied Cyber-security Research, Indiana University, Bloomington, IN, December 2, 2010.

"From Kinsey to Anonymization: Approaches to Preserving the Privacy of Survey Participants", Department of Mathematics and Computer Science, Emory University, Atlanta, GA, November 19, 2010; Indiana University, Bloomington, IN, November 12,2010.

"PlugNPlay Trust for Embedded Communications Systems", Purdue University, CERIAS, October 14, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Characterizing Trustworthy Behavior of Email Servers", CAARMS 2009, Rice University, June 23-26, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Hardware Enabled Access Control for Electronic Voting Systems", Rose Hulman, January 6, 2009; Jackson State University, February 26, 2009

"Hardware-enabled Access Control for the Prime III Voting System", Auburn University, June 16, 2008

"Understanding the Behaviors of Malicious Users of Pervasive Computing Environments", ARO/FSTC Workshop on Insider Attacks and Cyber Security, June 11-12, 2007, Arlington, Virginia.

"Trusting Your Security", Second Annual Network Security Workshop, Lehigh University, May 15-16, 2006

"Establishing a Trusted Computing Base for Software Defined Radio", Information Security Institute, Johns Hopkins University, February 2005, Baltimore, Maryland.

Invited Talks

"Towards a Framework for Automatically Satisfying Security Requirements", Department of Computer Science, Queens University, October 2004, Kingston, Ontario, Canada.

"Overlay QoS", Department of Computer Science, Auburn University, February 2004, Auburn, Alabama.
"Distributed Admissions Control for Sticky QoS", *Ninth Annual Conference for African-American Researchers in the Mathematical Sciences,* June 2003, West LaFayette, Indiana.

"Distributed Admissions Control for Sticky QoS". *Sixth Informs Telecommunications Conference,* March, 2002, Boca Raton, Florida.
Former Congressman Lee Hamilton, Professor Fred Cate, and Professor Raquel Hill, "Security and Privacy in a Cyberwar World: A conversation about Edward Snowden, the NSA and the outlook for reform", *Indiana Statewide IT Conference*, Indiana University, Bloomington, IN October, 29, 2013

Panels

R. Hill, "Building Trusting Systems: Trusting Your Security", *Workshop on Useable Security, co-located with 11th Conference on Financial Cryptography and Data Security*, February 2007, Lowlands, Scarborough, Trinidad/Tobago.

R. Hill, R. Campbell, "Understanding, Managing and Securing Ubiquitous Computing Environments", *Grace Hopper Celebration of Women in Computing*, October 2004, Chicago, Illinois.

C. Lester, R. Hill, M. Spencer, "Making Waves: Navigating the Transition from Graduate Student to Faculty Member", *Grace Hopper: Celebration of Women in Computing*, San Diego, California, Oct. 4-6, 2006.

Teaching

University	Course	Semesters Taught
Indiana University	I230 Analytical Foundations of Security	Spring 2006, Fall 2007-2011
	CSCI P438 Introduction to Computer Networks	Fall 2009,2010,2012
	CSCI H343 Data Structures (Honors	Fall 2011,2012
	CSCI B649 Trusted Computing	Spring 2006-2011
	CSCI B649 Data Protection	Spring 2013
Georgia Institute of Technology	ECE 2030 Introduction to Computer Engineering	Spring 2003, Summer 2003

Professional Activities

Member of Technical Program Committee

- IEEE International Conference on Information Technology (ITCC) 2005, Pervasive Computing Track
- IEEE International Conference on Communications 2006: Network Security and Information Assurance Symposium
- Indiana Women in Computing Conference February 2006
- Workshop on Security, Privacy and Trust for Pervasive Computing Applications, September 2006, 2007, 2008, 2009, 2010
- Middleware Support for Pervasive Computing Workshop (PERWARE) at the 4th Conference on Pervasive Computing and Communications, March 2007, 2008, 2009
- IEEE International Conference on Computer Communications and Networks, (ICCCN'06), Network Security and Dependability Track, October 2006; (ICCCN'07), Pervasive Computing and Mobile Networking Track, August 2007.
- IFIP Sixth International Conference on Networking (Networking 2007, 2008),
- Fourth International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, March 17-20, 2008 (Tridentcom 2008)
- First International ICST Conference on Mobile Wireless Middleware, Operating Systems and Applications, February 13-15, 2008, (Mobileware 2008, 2009,2010

Member of Review Panel

- **National Science Foundation**
- **Department of Energy**

Appendix B

Appendix B
Materials Considered or Relied Upon

IH Transcripts and Exhibits	**Bates Range**
13.02.05 Boyle, John - Transcript	FTC-000001-FTC-000115
13.02.05 Boyle, John - Exhibits	FTC-000116-FTC-000376
13.02.06 Daugherty, Michael - Transcript	FTC-000377-FTC-000416
13.02.06 Daugherty, Michael - Exhibit #8	FTC-000225-FTC-000246
13.02.06 Daugherty, Michael - Exhibit #14	FTC-000283-FTC-000304
13.02.06 Daugherty, Michael - Exhibit #23	FTC-000417-FTC-000423
13.05.02 Simmons, Alison - Transcript	FTC-000424-FTC-000493
13.05.02 Simmons, Alison - Exhibits	FTC-000494-FTC-000512
13.05.03 Kaloustian, Curt - Transcript	FTC-000513-FTC-000638
13.05.03 Kaloustian, Curt - Exhibits	FTC-000639-FTC-000656

Deposition Transcripts and Exhibits
14.01.09 Maire, Chris
14.01.10 Bureau, Matt
14.01.11 Brown, Sandra
14.01.13 Hudson, Lawrence
14.01.17 Maxey, Jerry Southeast Urology Network Rule 3.33
14.01.24 Howard, Patrick
14.04.28 Boyle, John
14.02.04 Randolph, Letonya Midtown Urology Rule 3.33
14.02.05 Simmons, Alison
14.02.06 Martin, Jeff
14.02.07 Gilbreth, Patricia
14.02.14 Bradley, Brandon
14.02.17 Carmichael, Lou
14.03.04 Daugherty, Michael LabMD Rule 3.33
14.02.10 Daugherty, Michael
14.01.25 Garrett, Karalyn
14.02.21 Harris, Nicotra
14.02.11 Parr, Jennifer
14.01.31 Sandrev, Peter Cypress Communication Rule 3.33
14.02.27 Truett, Allen
13.12.02 Dooley, Jeremy
13.11.21 Boback, Robert Tiversa Rule 3.33
13.12.13 Hyer, Robert

Correspondence	**Bates Range**
10.02.24 Ellis Letter	FTC-LABMD-002506-FTC-LABMD-002520
10.06.04 Ellis Letter	FTC-LABMD-002523-FTC-LABMD-002524
10.07.16 Ellis Letter	FTC-LABMD-002495-FTC-LABMD-002503
10.07.16 Ellis Exhibits	FTC-LABMD-002505-FTC-LABMD-003131

10.08.30 Ellis Letter	FTC-LABMD-003132-FTC-LABMD-003137
10.08.30 Ellis Exhibits	FTC-LABMD-003138-FTC-LABMD-003270
11.05.16 Rosenfeld Letter	FTC-LABMD-003445-FTC-LABMD-003452
11.05.16 Rosenfeld Exhibits	FTC-LABMD-003453-FTC-LABMD-003628
11.05.31 Rosenfeld Letter	FTC-LABMD-003629-FTC-LABMD-003634
11.05.31 Rosenfeld Exhibits	FTC-LABMD-003635-FTC-LABMD-003748
11.07.22 Rosenfeld Email	FTC-LABMD-003749-FTC-LABMD-003750
11.07.22 Rosenfeld Email	FTC-LABMD-003756-FTC-LABMD-003756
11.07.22 Rosenfeld Email-Screenshots	FTC-LABMD-003757-FTC-LABMD-003761
11.12.21 CID to Daugherty and Responses	FTC-000417-FTC-000423
13.01.17 CID to Daugherty and Responses	NA
11.12.21 CID to LabMD and Responses	FTC-000116-FTC-000127
13.01.17 CID to LabMD and Reponses	NA

Documents Produced by LabMD

FTC-LABMD-000001-FTC-LABMD-000304
FTC-LABMD-000306-FTC-LABMD-000385
FTC-LABMD-000388-FTC-LABMD-000603
FTC-LABMD-000605-FTC-LABMD-000634
FTC-LABMD-000636-FTC-LABMD-000646
FTC-LABMD-000648-FTC-LABMD-000776
FTC-LABMD-003139-FTC-LABMD-003444
FTC-LABMD-003453-FTC-LABMD-003628
FTC-LABMD-003635-FTC-LABMD-003748
FTC-LABMD-003752-FTC-LABMD-003761
FTC-LABMD-003763-FTC-LABMD-004358
FTC-LABMD-004514-FTC-LABMD-004536
FTC-LABMD-004576-FTC-LABMD-004677
FTC-LABMD-004782-FTC-LABMD-004851
FTC-LABMD-004882-FTC-LABMD-004891
FTC-LABMD-004897-FTC-LABMD-004906
FTC-LABMD-004922-FTC-LABMD-004950
FTC-LABMD-004975-FTC-LABMD-005129
FTC-LABMD-005160-FTC-LABMD-005221
FTC-LABMD-005250-FTC-LABMD-005310
FTC-LABMD-005644-FTC-LABMD-005651
FTC-LABMD-005686-FTC-LABMD-006637
FTC-LABMD-006820-FTC-LABMD-006823
FTC-LABMD-006828-FTC-LABMD-006835
FTC-LABMD-007128-FTC-LABMD-007132
FTC-LABMD-007212-FTC-LABMD-007342
FTC-LABMD-007463-FTC-LABMD-007507
FTC-LABMD-007619-FTC-LABMD-007627
FTC-LABMD-007636-FTC-LABMD-007659
FTC-LABMD-007990-FTC-LABMD-007994
FTC-LABMD-008022-FTC-LABMD-008036

FTC-LABMD-008108-FTC-LABMD-008124
FTC-LABMD-008780-FTC-LABMD-008783
FTC-LABMD-009955-FTC-LABMD-009958
FTC-LABMD-009960-FTC-LABMD-010060
FTC-LABMD-010513-FTC-LABMD-010615
FTC-LABMD-010654-FTC-LABMD-010660
FTC-LABMD-011103-FTC-LABMD-011106
FTC-LABMD-011116-FTC-LABMD-011120
FTC-LABMD-011855-FTC-LABMD-011858
FTC-LABMD-012751-FTC-LABMD-012755
FTC-LABMD-013286-FTC-LABMD-013289
FTC-LABMD-013304-FTC-LABMD-013308
FTC-LABMD-013441-FTC-LABMD-013448
FTC-LABMD-014422-FTC-LABMD-014483
FTC-LABMD-014512-FTC-LABMD-014521
FTC-LABMD-014533-FTC-LABMD-014607
FTC-LABMD-014613-FTC-LABMD-014620
FTC-LABMD-014625-FTC-LABMD-014680
FTC-LABMD-014689-FTC-LABMD-014692
FTC-LABMD-014699-FTC-LABMD-014869
FTC-LABMD-014896-FTC-LABMD-014952
FTC-LABMD-014957-FTC-LABMD-015016
FTC-LABMD-015020-FTC-LABMD-015218
FTC-LABMD-015242-FTC-LABMD-015245
FTC-LABMD-015414-FTC-LABMD-015430
FTC-LABMD-015457-FTC-LABMD-015477
FTC-LABMD-015491-FTC-LABMD-015525
FTC-LABMD-015542-FTC-LABMD-015962
FTC-LABMD-015994-FTC-LABMD-016063
FTC-LABMD-016135-FTC-LABMD-016141
FTC-LABMD-016148-FTC-LABMD-016179

Documents Produced by Tiversa
TIVERSA-FTC RESPONSE-000001-006904

Documents Produced by Sacramento Police Department
FTC-SAC-000001-FTC-LABMD-000044

Documents Produced by the Privacy Institute
FTC-PRI-000001-FTC-PRI-001719

Documents Produced by Cypress Communication, LLC
FTC-CYP-000001-FTC-CYP-000001
FTC-CYP-0001656-FTC-CYP-0001725
FTC-CYP-0001729-FTC-CYP-0001733
FTC-CYP-0001735-FTC-CYP-0001757

FTC-CYP-0001759-FTC-CYP-0001763
FTC-CYP-0001765-FTC-CYP-0001772
FTC-CYP-0001784-FTC-CYP-0001811
FTC-CYP-0001881-FTC-CYP-0001896
FTC-CYP-0001898-FTC-CYP-0001899
FTC-CYP-0001954-FTC-CYP-0001968
FTC-CYP-0001973-FTC-CYP-0001976
FTC-CYP-0001983-FTC-CYP-0001984
FTC-CYP-0002008-FTC-CYP-0002009
FTC-CYP-0002109-FTC-CYP-0002109

Documents Produced by ProviDyn, Inc.
FTC-PVD-000001-FTC-PVD-001582

Documents Produced by TrendMicro
FTC-TRM-000001-FTC-TRM-000455

Web Content Considered or Relied Upon

- The Center for Information Security Awareness, http://www.cfisa.org/, last accessed March 18, 2014.
- Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host, http://stealth.sourceforge.net/, last accessed March 16, 2014.
- The Computer Emergency Response Team (CERT), https://www.cert.org/, last accessed March 18, 2014.
- The Computer Emergency Response Team (CERT) -- Anonymous FTP Activity (1997), http://www.cert.org/historical/advisories/CA-1993-10.cfm, last accessed March 18, 2014.
- Cisco -- Cisco 1841 Integrated Services Router, http://www.cisco.com/c/en/us/products/routers/1841-integrated-services-router-isr/index.html, last accessed March 16, 2014.
- Common Vulnerabilities and Exposures – The Standard for Information Security Vulnerability Names, http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0527, last accessed March 16, 2014.
- Federal Communications Commission -- Cybersecurity for Small Businesses, http://www.fcc.gov/cyberforsmallbiz, last accessed March 16, 2014.
- Microsoft Forum -- Disable SSL v2 in IIS6?, http://forums.iis.net/t/1131343.aspx, last accessed March 16, 2014.
- Microsoft News Center -- Microsoft Windows Server 2003 Is Available Worldwide Today (April 24, 2003), http://www.microsoft.com/en-us/news/press/2003/apr03/04-24windowsserver2003launchpr.aspx, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Security TechCenter – Security Guidance for IIS, http://technet.microsoft.com/en-us/library/dd450371.aspx, last accessed March 16, 2014.

- Microsoft Security TechCenter – Microsoft Security Advisory (2661254), http://technet.microsoft.com/en-us/security/advisory/2661254, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Support – How to disable simple file sharing and how to set permissions on a shared folder in Windows XP, http://support.microsoft.com/kb/307874, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/?id=187498, last accessed March 16, 2014.
- Microsoft Support – How to install and use the IIS Lockdown Wizard, http://support.microsoft.com/kb/325864, last accessed March 16, 2014.
- Microsoft Support – Microsoft Security Advisory: Update for minimum certificate key length, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Multi-State Information Sharing & Analysis Center – Cyber Security Awareness Free Training and Webcasts, http://msisac.cisecurity.org/resources/videos/free-training.cfm, last accessed March 18, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2611, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3509, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2002-1717&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5969, last accessed March 16, 2014.

- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1491, Last accessed March 16, 2014.
- Nmap.org – www.nmap.org, last accessed March 18, 2014.
- Open Source SECurity, http://www.ossec.net/, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/76, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/show/osvdb/193, last accessed March 16, 2014.
- Symantec - Symantec Backup Exec for Windows Server: PRC Interface Heap Overflow, Denial of Service, http://securityresponse.symantec.com/avcenter/security/Content/2007.07.11a.html, last accessed March 17, 2014.
- Symantec – VERITAS Backup Exec for Windows Servers, VERITAS Backup Exec for NetWare Servers, and NetBackup for NetWare Media Server Option Remote Agent Authentication Vulnerability, http://securityresponse.symantec.com/avcenter/security/Content/2005.08.12b.html, last accessed March 17, 2014.
- The SysAdmin Audit Network Security Institute (SANS) – Information Security Resources, http://www.sans.org/security-resources/, last accessed March 18, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/crck_vista.b, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/Malware.aspx?id=35451&name=CRCK_KEYGEN&language=au, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/CRCK_KEYGEN.AU, last accessed March 16, 2014.
- U.S. Department of Health and Human Services – Health Information Privacy: The Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, last Accessed March 18, 2014.

Articles & Publications

- Espenschied, Jon, "Five free pen-testing tools" (May 27, 2008), http://www.computerworld.com/s/article/9087439/Five_free_pen_testing_tools, last accessed March 16, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.
- Halamka, John D., Szolovits, Peter, Rind, David, Safran, Charles, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information" Journal of the American Medical Informatics, (Nov-Dec 1997), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC61263/, last accessed March 16, 2014.

- Houston, Peter, "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www.microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.
- Kelly, Allen, "Proper Management of SSL Certificates: Why it is Critical to Your Organization - Part II" (September 8, 2011), http://www.symantec.com/connect/blogs/proper-management-ssl-certificates-why-it-critical-your-organization-part-ii, last accessed March 16, 2014.
- Kissel, Richard, "Small Business Information Security: The Fundamentals" (October 2009), http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf, last accessed March 16, 2014.
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments" (September 18, 2012), http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf, last accessed March 18, 2014.
- PCI Security Standards Council "PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1" (September 2006), https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf, last accessed March 18, 2014.
- SANS Institute InfoSec Reading Room, "Understanding IIS Vulnerabilities - Fix Them!" (2001), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute InfoSec Reading Room, "Cryptanalysis of RSA: A Survey" (2003), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343, last accessed March 18, 2014.
- Stoneburner, Gary, Goguen, Alice, Feringa, Alexis, "NIST Risk Management Guide for Information Technology Systems" NIST (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, last accessed March 18, 2014.
- U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf, last accessed March 18, 2014.
- Wagner, David, Schneier, Bruce, "Analysis of the SSL 3.0 protocol," https://www.schneier.com/paper-ssl.pdf, last accessed March 16, 2014.
- Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf, last accessed March 18, 2014.

Books

- Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional (1995).

- National Research Council, "For the Record: Protecting Electronic Health Information" Washington, DC: The National Academies Press (1997), http://www.nap.edu/openbook.php?record_id=5595&page=R1, last accessed March 16, 2014.

FTC Provided Documents

- 13.08.28 Complaint
- 14.02.19 Complaint Counsel's Requests for Admission to Respondent LabMD
- 14.02.20 Revised Answer to Complaint Counsel's Interrogatory 1 and 2
- 14.03.03 Respondent's Objections and Responses to Complaint Counsel's Requests for Admission
- 14.03.10 Order Granting In Part and Denying In Part Complaint Counsel's Motion for Discovery Sanctions
- 14.03.14 Order on Complaint Counsel's Motion for Discovery Responses
- 14.03.17 Respondent's Supplemental Response to Complaint Counsel's First Set of Interrogatories

Miscellaneous

- Federal Register, Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information" (October 15, 2002), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt, last accessed March 18, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.

EXHIBIT 16

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 17

Report of Rick Kam, CIPP/US

In the Matter of LabMD

FTC Complaint #1023099, Docket #9357

March 18, 2014

Table of Contents

TABLE OF CONTENTS 2
EXECUTIVE SUMMARY 3
INTRODUCTION 3
II. SUMMARY OF THE FTC'S REQUEST FOR EXPERT OPINION 5
III. SUMMARY OF CONCLUSIONS 8
IV. IDENTITY CRIME: AN OVERVIEW 10
V. IMPACT OF IDENTITY CRIMES ON VICTIMS 13
VI. ANALYSIS OF RISK OF HARM FROM LABMD'S FAILURE TO PROTECT CONSUMER DATA 17
APPENDIX A: CV 25
APPENDIX B: LITERATURE REVIEW 33
APPENDIX C: STATE BREACH NOTIFICATION LAWS IN EFFECT BEFORE MAY 2008 37
APPENDIX D: LIST OF CPT CODES 39

practices. ID Experts provided case studies of identity crimes to an analytical repository of identity threats and counter measures called *Identity Threat Assessment and Prediction* (ITAP). (2009 - present)

- Member of the International Association for Privacy Professionals (IAPP), the most comprehensive, member-based privacy community and resource. I maintain a Certified Information Privacy Professional CIPP/US certification for data privacy. (2010 - present)

- Member of Healthcare Information and Management Systems Society (HIMSS), a global, member-based non-profit focused on the betterment of healthcare information technology. (2010 - present)

- Member of the Health Care Compliance Association, (HCCA), a member-based non-profit that provides training, certification and resources in support of ethics and regulatory compliance in healthcare. (2011- present)

- Founding member of the Medical Identity Fraud Alliance (MIFA), a group of over 40 private and public industry members in the fight against medical identity theft and medical fraud. (2013 - present)

I have attached a copy of my CV, which fully describes my background and qualifications, and includes a list of my publications over the last 10 years (see Appendix A).

Compensation

The FTC has engaged me as an expert witness in support of its complaint against LabMD. The compensation for this work is $350 per hour, and this report and my testimony are based on the experience outlined in this section, a literature review (see Appendix B), and documents I received from the FTC.

II. Summary of the FTC's Request for Expert Opinion

The Federal Trade Commission has asked me to assess the risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information. For the purposes of my analysis, I have assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks.

FTC Documents for Analysis

I have based my analysis on my experience as outlined in Section I of this report, a literature review (see Appendix B), and the documents that I received and reviewed from the FTC, which are listed here.

Documents related to the P2P Disclosure

- **P2P Insurance Aging file (insuranceaging_6.05.071.pdf):** This is the 1,718-page file Tiversa discovered on a peer-to-peer (P2P) network that contained consumer data from the LabMD Insurance Aging Report with roughly 9,300 records. The data elements included in this file are:
  - First and last names, and middle initials
  - Dates of birth
  - Nine-digit Social Security numbers (SSNs)
  - Health insurance provider numbers, names, addresses, and phone numbers
  - Current Procedural Terminology (CPT) Codes: Uniform set of codes defined by the American Medical Association to describe medical, surgical, and diagnostic services.
  - Billing dates and amounts

- **Transcript of the deposition of Robert Boback, CEO of Tiversa, dated November 21, 2013, with supporting exhibits.**

- **Transcript of the deposition of Alison Simmons, former LabMD IT employee, dated February 5, 2014, with supporting exhibits.**

- **Transcript of the deposition of Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt University, dated February 18, 2014, with supporting exhibits.**

- **Transcript of the deposition of Michael Daugherty, President and CEO of LabMD, dated March 4, 2014.**

Documents related to the Sacramento Disclosure

- **Day Sheets from LabMD (Sacramento LabMD-Documents.pdf):** These are documents the Sacramento Police Department found on October 5, 2012, during an arrest of two individuals who pleaded "no contest" to identity theft charges. The Day Sheets contain approximately 600 records with first and last names, and middle initials; nine-digit Social Security numbers; and billing dates and amounts.

- **2011.05.31 Rosenfeld Letter to the FTC**
- **2011.07.12 Rosenfeld Email to the FTC**
- **FTC-MID-000012:** 1/6/14 letter regarding LabMD not "accepting new specimens."
- **FTC Complaint in the Matter of LabMD**
- **Protective Order Governing Discovery of Material.pdf**
- **LabMD's Objections to and Responses to Complaint Counsel's Requests for Admission, dated March 3, 2014**
- **LabMD's Responses to Complaint Counsel's Interrogatories and Discovery Requests, dated March 3, 2014**

III. Summary of Conclusions

As consumers, we place trust in the organizations that hold our most sensitive personal information: Social Security numbers, financial data, and our medical history, to name a few. We have confidence that they will protect this information from unauthorized disclosure.

Once a consumer's sensitive personal data is disclosed without authorization, that consumer has no control over who accesses this information, thus becoming vulnerable to identity fraud, identity theft, and medical identity theft. These crimes can damage a consumer's economic well-being and reputation, and even risk his or her health. Medical identity theft can be especially difficult to resolve because it is impossible to make a victim's personal medical history private again.

In Sections V and VI of this report, I provide an overview of the impact of identity crime, with an emphasis on medical identity theft, and illustrate the possible harm to victims of these crimes. Then, based on that information, the FTC-provided documents, the literature review (see Appendix B), and my own expertise and experience, I provide my analysis of the LabMD case, specifically:

- That consumers have no way of knowing about certain unauthorized disclosures of their sensitive personal information, including medical information, thus putting them at risk of possible harms from identity crimes, including medical identity theft.

- That use of a consumer's SSN by other people with different names is an indication that identity thieves may have used the consumer's SSN.

- That LabMD's failure to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information is likely to cause substantial harm, including harm stemming from medical identity theft.

Summary of LabMD Analysis

In my opinion, LabMD's failure to provide reasonable and appropriate security for sensitive personal information, including medical information, is likely to cause substantial injury to consumers and puts them at significant risk of identity crimes. The following is a summary of my analysis of likely risks of harm from identity theft and medical identity theft to the approximately 10,000 consumers affected by the P2P and Sacramento disclosures. Apart from these two incidents, I also believe that LabMD's failure to provide reasonable and appropriate security for the more than 750,000 consumers' personal information maintained on its computer networks creates a risk of unauthorized disclosure of this information. These unauthorized disclosures and the failure to provide reasonable and appropriate security are likely to cause substantial harm to these consumers.

P2P Disclosure

- Approximately 9,300 consumers from the May 2008 unauthorized disclosure are at significant risk of harm from identity crimes.

- LabMD did not notify the 9,300 consumers whose personal information was contained in the 1,718-page P2P Insurance Aging file that Tiversa discovered on February 5, 2008. Robert Boback indicated in his testimony on November 21, 2013, that this file was found on peer-to-peer networks. He indicated that at four of the IP addresses on which Tiversa found the 1,718-page P2P Insurance Aging file, Tiversa also found unrelated sensitive consumer information that could be used to commit identity theft, including passwords, tax returns, account numbers, and Social Security numbers.

- These 9,300 consumers have had no opportunity to mitigate the risk of harm because LabMD, which has known about the unauthorized disclosure of their personal information since May 2008, has not notified them of this disclosure. Even if LabMD had provided notice, consumers would still remain at risk of harm from identity crimes since this unauthorized disclosure included Social Security numbers and health insurance numbers, which can be used to commit identity crimes over an extended period of time.

- There is a significant risk of reputational damage for 3,000 or more consumers from the unauthorized disclosure of sensitive medical information, specifically diagnostic codes indicating tests for prostate cancer, herpes, hepatitis, HIV, and testosterone levels.

1. The nature and extent of the sensitive personal information involved, including the types of identifiers and the likelihood of re-identification. In other words, could the disclosed consumer data elements be used to facilitate identity theft, identity fraud, and medical identity theft? Was sensitive personal data part of the unauthorized disclosure (e.g., name, medical records, health insurance number, diagnostic codes)?

2. The unauthorized person who used the protected health information or to whom the disclosure was made. For instance, was this an employee disclosing the information to another employee, which poses a low risk, versus to an unauthorized individual not associated with that entity, be it another consumer, business, identity thief, etc.?

3. Whether the sensitive personal information was actually acquired or viewed. An example: Was the information stored on a secure encrypted device such as a laptop or storage drive, or were they paper health records left on a public bus and viewed by others?

4. The extent to which the risk to the protected health information has been mitigated. For instance: Were copies of sensitive information destroyed during its recovery from unauthorized parties, or is the data still available for others to misuse?

Analysis of the P2P Disclosure (9,300 records)

According to the materials supplied by the FTC, Tiversa alerted LabMD of the unauthorized disclosure of the P2P Insurance Aging file that contained 9,300 consumer records in May 2008. The compromised data included:

- First and last names, and middle initials
- Dates of birth
- Nine-digit Social Security numbers
- Health insurance provider numbers, names, addresses, and phone numbers
- Current Procedural Terminology (CPT) diagnostic codes
- Billing dates and amounts

I analyzed these data elements looking at the first risk factor, specifically the nature and extent of the information disclosed. Approximately 9,300 consumers' sensitive data was found in a LabMD document available on a P2P network on February 5, 2008, in clear text, according to Robert Boback's testimony. The disclosure of names with corresponding Social Security numbers, health insurance provider numbers, and CPT diagnostic codes pose a greater risk of various identity crimes.

The second and third risk factors consider to whom the disclosure was made and whether the information was acquired and viewed. In his testimony, Boback said that the P2P Insurance Aging file was found at four IP address along with unrelated sensitive consumer information that could be used to commit identity theft. Boback also testified sensitive consumer information in the P2P file could be available to anyone who had access to the peer-to-peer network. He also stated that law enforcement had apprehended someone suspected of identity theft or fraud using one of the IP addresses.

The fourth risk factor is the extent to which the risk to a consumer's personal information has been mitigated. According to Boback's testimony, the P2P Insurance Aging file was first found on the peer-to-peer network on February 5, 2008, at IP address 68.107.85.250. It was found again on November 5, 2008, at IP address 173.16.83.112; again on April 7, 2011, at IP address 201.194.118.82; and yet again on June 9th in 2011, at IP address 90.215.200.56. Boback also said Tiversa searched for the file in preparation for his testimony on November 21, 2013, and still found the file available on the P2P network. LabMD did not mitigate the risk of identity crimes created by this unauthorized disclosure by notifying consumers. In my experience, a significant number of these consumers have or could still fall victim to identity crimes since they have no way of independently knowing that LabMD disclosed their information without authorization almost 6 years ago. This unauthorized disclosure puts the affected consumers at a significantly higher risk of identity crimes than the general public.

Harm from P2P Disclosure

Estimated Financial Out-of-Pocket Cost to Victims of Medical Identity Theft

According to the findings from the 2013 Survey on Medical Identity Theft by Ponemon Institute, 0.0082 is the estimated base rate for medical identity theft in the U.S.[16] This represents the proportion of consumers who indicated that they were medical identity theft victims, as drawn from a representative panel of 5,000 adult-aged U.S. consumers.[17]

Therefore:

9,300 breached records x 0.0082 = 76, the estimated number of victims for medical identity theft.

The Ponemon study also found that 36 percent of victims of medical identity theft paid an average of $18,660 in out-of-pocket costs.

---

[16] Ponemon 2013 Survey on Medical Identity Theft, p. 2.

[17] Ponemon 2013 Survey on Medical Identity Theft, p. 27.

EXHIBIT 18

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**DOCKET NO. 9357**
	)	
	)	**PUBLIC**
LabMD, Inc.,	)	
a corporation.	)	

DECLARATION OF LabMD, INC. PRESIDENT AND CHIEF EXECUTIVE OFFICER MICHAEL J. DAUGHERTY IN SUPPORT OF RESPONDENT LabMD, INC.'s APPLICATION FOR STAY OF ORDER PENDING REVIEW IN U.S. COURT OF APPEALS

I, Michael J. Daugherty, in my capacity as President and Chief Executive Officer ("CEO") of Respondent LabMD, Inc. ("LabMD"), declare under penalty of perjury that the following is true and correct to the best of my knowledge, information, and belief:

1. I am over eighteen (18) years of age, and the following facts are based on my own personal knowledge and, if called as a witness, I could and would testify competently to them.

2. I am the President and CEO of LabMD.

3. In mid-January 2014, LabMD began winding down operations and stopped accepting specimens for testing and stopped performing testing on specimens in its possession.

4. LabMD does not have any employees. Beginning in March 2014, LabMD had one employee. Since July 2016, LabMD has had no employees.

5. LabMD does not generate any revenue. LabMD has not generated revenue from testing since January 2014.

6. LabMD is not a profitable enterprise and is losing money.

   a. In the 2015 Tax Year alone, for example, LabMD had an ordinary business loss of $310,243.00.

   b. LabMD's assets are minimal and de minimis. For example, LabMD has less than $5,000 available in cash.

   c. LabMD's liabilities and judgments against it far exceed its nominal assets, and LabMD is already insolvent.

   d. It is highly unlikely, if not impossible, that LabMD will ever become solvent again.

7. With the exception of records LabMD is required to retain by law, devices used to store such records, and a minimal amount of office equipment (for example, a printer and fax machine), LabMD does not own any property. In 2014, the vast majority of LabMD's property, such as diagnostic testing equipment, was utilized to satisfy LabMD's debt obligations.

8. After LabMD ceased operations, LabMD had to give up the space it leased to perform testing on specimens. LabMD subsequently became involved in a dispute with the landlord over early termination of the lease. At this time, there is an approximately $1,000,000.00 judgment pending against LabMD relating to this early termination. Legal proceedings are ongoing.

9. At this time, LabMD does not have an operational computer network (*i.e.*, LabMD does not have one or more computers and/or other electronic devices that are turned on or connected to one another and/or the Internet) containing any "Personal Information," as defined in the Final Order of the Federal Trade Commission ("Commission") dated July 28, 2016. LabMD has not had an operational computer network since July 2014.

10. LabMD's operations are limited to preserving tissue samples and medical records for LabMD's former physician clients upon request.

11. All "Personal Information," as defined by the Final Order of the Commission, is currently stored using the following physical, administrative, and other safeguards and security mechanisms:

    a. LabMD's computer systems are stored in a locked room in a secure location.

    b. I am the only person who has a key to the locked room in which LabMD's computer systems are stored and am the only person who is authorized to access that room.

    c. Even if someone managed to determine the location of that locked room, break into it, and/or manage to remove LabMD's computer systems from the secure location, in order to access the "Personal Information," as defined by the Commission Final Order, he or she would have to not only know how to operate this equipment but also defeat the password-protection security features, as well as networking features in rebuilding database software functions.

12. No "Personal Information," as defined by the Commission Final Order, is stored in electronic form on any device (for example, a computer or server) that is connected to the Internet.

13. LabMD has a legal obligation to retain such information for a period of ten (10) years, pursuant to Georgia state law. My understanding is that such information is also Protected Health Information ("PHI") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), as well as United States Department of Health and Human Services ("HHS") regulations implementing those statutes.

14. I have no expectation that LabMD will ever resume business or create an operational computer network containing "Personal Information" subject to the Commission Final Order and connected to the Internet, and I do not see how these things could ever happen, but in no event would LabMD do these things until LabMD's petition for review of this matter and the Commission Final Order has been fully adjudicated.

15. Except as stated in paragraphs 17-18 of this Declaration, no "Personal Information," as defined by the Commission Final Order, is stored in electronic form on any device (for example, a computer or server) that is plugged in to an electric socket and turned on.

16. LabMD does not expect ever to turn on its computers, servers, and/or other electronic devices containing "Personal Information," as defined by the Order except as stated in paragraphs 17-18 of this Declaration, and does not see how that would ever happen; and in no event will LabMD do so, before LabMD's petition for review of this matter and the Commission Final Order has been fully adjudicated or unless needed to fulfill a physician request. Likewise, LabMD does not expect ever to connect such devices to the Internet and does not see how that would ever happen, and it will in no event do so until LabMD's petition for review of this matter and the Commission Final Order has been fully adjudicated.

17. Consistent with LabMD's legal obligation to maintain medical records, discussed above, LabMD continues to possess its "Lytec" server, on which records for referring physicians' patients who received tests are stored.

18. On request, LabMD provides its former clients (physicians) with copies of medical records stored on its server.

    a. To do this, LabMD physically plugs in these electronic devices solely for the purpose of retrieving information specifically requested by physicians.

b. LabMD prints physical hard copies of the requested information to either mail or send via facsimile to the physician.

c. Afterwards, LabMD immediately turns off and unplugs the servers.

d. At no point are these devices connected to or accessible via the Internet.

19. LabMD does not expect ever to resume operations and does not see how that could ever happen, and in no event would LabMD even attempt to resume operations until LabMD's petition for review of this matter and the Commission Opinion and Final Order has been fully adjudicated by a United States Court of Appeals and/or the United States Supreme Court.

20. If LabMD ever did resume operations, even though it does not expect that to happen and does not see how it ever could happen, it is my understanding that LabMD would be required to comply with data security standards set by HIPAA and HITECH, as well as HHS regulations implementing those statutes.

21. I have reviewed the Commission's July 28, 2016 Opinion and Final Order.

22. The Commission Final Order contains provisions that, as a condition of compliance, will require LabMD to incur substantial and unrecoverable monetary and nonmonetary compliance costs. Examples of such substantial and unrecoverable monetary and nonmonetary compliance costs include but are not limited to the following:

a. Part I of the Commission Final Order requires LabMD to "establish and implement" a "comprehensive information security program."

i. The Commission Opinion appears to direct LabMD to consult and study it, as well as "guidance" issued by NIST and a private organization known as "the SANS Institute," to determine how the Commission will or may later interpret Part I of the Commission Final Order.

ii. LabMD does not know what the Commission believes now (or will later claim) constitutes a "comprehensive information security program," which in its view is sufficiently "reasonably designed to protect the security, confidentiality, and integrity of personal information[.]"

iii. LabMD does not know what the Commission believes now (or will later claim) are "administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers."

iv. In order to even attempt to adopt a "comprehensive information security program" that complies with the Final Order, as interpreted by the Commission, LabMD must consult with (and pay) Information Technology ("IT") professionals and attorneys to work with LabMD to conduct a risk assessment, documented in writing, to attempt to determine what Part I of the Final Order (as informed by the Commission Opinion, materials disseminated by the SANS Institute, NIST, and other sources) requires.

v. LabMD does not know whether the Commission may interpret Part I of the Final Order to require LabMD to purchase additional equipment. For instance, if Part I is interpreted to require the rebuilding of LabMD's computer network, my understanding is that this will cost at least $10,000.00 plus maintenance fees.

vi. LabMD does not know and cannot determine with ascertainable certainty the extent to which the Commission may interpret Part I of the Final Order to

require or prohibit medical data security practices that are inconsistent with, in addition to, and/or otherwise different from those that are either required or addressable under HIPAA and HHS regulations, such as the HIPAA Security Rule, establishing medical-industry-specific data security standards.

b. Part II of the Commission Final Order requires LabMD to obtain initial biennial assessments and reports from third-party contractors holding certain certifications and qualifications. It is my understanding that LabMD is required to pay for such third-party assessments. I have been told that such assessments can cost in the neighborhood of $250,000.00.

c. Part III of the Commission Final Order appears to require LabMD to send via first class mail a notification to thousands of people and their health insurance companies, as well as make reasonable efforts to find such mailing addresses by conducting Internet research.

   i. Among other things, this will require LabMD to pay for stamps, envelopes, and paper, as well as set up and pay for a toll-free telephone number.[1]

   ii. In addition, performing tasks required by Part III of the Final Order will require substantial time and effort. For instance, to the extent Part III refers to the 1718 File, LabMD will need to either pay a third party to handle the logistical requirements of mailing thousands of letters (including placing stamps on said letters, addressing such letters to proper recipients, and placing letters in envelopes), or I will need to do this by myself.

---

[1] According to the United States Postal Service ("USPS") website, https://www.usps.com/ship/first-class-mail.htm , the price of a "First-Class Mail Forever® Stamp is $0.47."

iii. LabMD also would need to respond to inquiries relating to the notification letters and conduct research sufficient to satisfy the Commission's unspecified definition of "reasonable efforts to find such mailing addresses," which, at minimum, appears to require me to "review[] online directories" or hire a third-party contractor to do so at substantial expense.

iv. Complying with Part III of the Final Order will require LabMD to determine how the Commission believes its definition of "Affected Individual" should be interpreted as applied to LabMD. This requires LabMD to determine what "reason to believe, was, or could have been, accessible to unauthorized persons" means. LabMD does not know how the Commission interprets this or how the Commission may later claim it should be interpreted.

v. Assuming that each stamp costs $0.47, the cost of stamps to notify referring physicians' patients listed on the 1718 File alone will be about $ 4,371.00, excluding the cost of stamps to notify the health insurance companies of this number of people, as well as the cost of paper, envelopes, time and labor, and the like. LabMD has calculated approximately 688 insurance companies for the individuals in the 1718 File alone.

d. Part VII of the Commission Final Order requires LabMD to submit a written report to the Commission "setting forth in detail the manner and form of their compliance with this order." LabMD will need to pay attorney(s) and IT professionals to assist in the preparation of such a report. I have been informed that this will cost about $20,000.00.

23. LabMD does not want to and cannot incur substantial compliance costs mandated by the Commission Final Order. Since LabMD is already insolvent, as discussed above, LabMD has no ability to pay the costs it would necessarily incur to even attempt to comply with the Commission Final Order. But for the Commission Final Order, LabMD would not incur such unpayable costs and I would use the time I would otherwise need to spend performing the tasks mandated by the Commission Final Order in a different way.

24. As stated above, Part III of the Commission Final Order appears to require LabMD to provide a government-ordered and government-approved notice to thousands of individuals and their health insurance companies. LabMD does not wish to engage in this government-mandated speech and disagrees in whole or in part with the content of the required notice.

25. LabMD believes that the content of the notification letters required by Part III of the Commission Order will also harm LabMD's reputation and lead to loss of good will toward LabMD.

26. LabMD asserts that the execution, delivery, and content of the notification letters required by Part III of the Commission Final Order will irredeemably and irretrievably cause direct and indirect harm, prejudice, and damage to the appeal rights guaranteed to LabMD by Congress pursuant to 15 U.S.C. §§ 45(c)-(d)

27. Attached hereto as Exhibit A is a true and correct copy of an excerpt from Plaintiff's Motion to Stay, filed on July 20, 2016, in the Court of Common Pleas of Allegheny County, Pennsylvania, in *Boback v. LabMD et al.*, Civil Division No. GD-14-016497.

28. Attached hereto as Exhibit B is a true and correct copy of an excerpt from the transcript of a Motions Hearing held on Thursday, August 25, 2016, in the Court of Common Pleas of

Allegheny County, Pennsylvania, in *Boback v. LabMD et al.*, Civil Division No. GD-14-016497.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on August 30, 2016

Michael J. Daugherty
President and Chief Executive Office
LabMD, Inc.

EXHIBIT A

IN THE COURT OF COMMON PLEAS OF ALLEGHENY COUNTY, PENNSYLVANIA

ROBERT J. BOBACK,	)	CIVIL DIVISION
	)	
Plaintiff,	)	GD-14-016497
	)	
v.	)	**MOTION TO STAY**
	)	
LABMD, INC., MICHAEL J. DAUGHERTY, and RICHARD EDWARD WALLACE,	)	Filed on behalf of Plaintiff, Robert J. Boback
	)	
Defendants.	)	Counsel of Record for This Party:
	)	
	)	Robert J. Ridge Pa. I.D. No. 58651
	)	
	)	Brandon J. Verdream Pa. I.D. No. 204162
	)	
	)	CLARK HILL PLC One Oxford Centre 301 Grant Street, 14th Floor Pittsburgh, PA 15219-1425 (412) 394-7711

B. Pending FBI Criminal Investigation

8. On March 1, 2016, the FBI executed a search warrant at Tiversa's offices in Pittsburgh.

9. Boback has not been provided direct information concerning the nature of the FBI's investigation and/or its reason for raiding Tiversa's office.

10. However, upon information and belief, the FBI's investigation concerns alleged false statements made to the Government, which are the same issues that are present in the instant matter. *See* Reuters Report attached hereto as "Exhibit A."

11. To the best of Boback's knowledge, the FBI investigation stemming from its raid of Tiversa's offices is ongoing.

C. Requested Relief

12. Based on the foregoing, Boback requests that the Court impose a temporary stay with respect to the instant matter for 120 days in order to allow for the FBI's criminal investigation to proceed unimpeded while Boback preserves his constitutional privileges.

II. ARGUMENT

13. '"The power to stay proceedings is incidental to the power inherent in every court to control the disposition of the causes on its docket with the economy of time and effort for itself, for counsel, and for litigants. How this can best be done calls for the exercise of judgment, which must weigh competing interests and maintain an even balance.'" *In re Adelphia Comms. Secs. Litig.*, 2003 U.S. Dist. LEXIS 9736, *5-6 (E.D. Pa. 2003) (quoting *Landis v. North American Co.*, 299 U.S. 248, 254-55 (1936)).

14. "A court has discretion to stay a case if the interests of justice require it." *Walsh Secs., Inc. v. Cristo Prop. Mgmt.*, 7 F. Supp. 2d 523, 526 (D.N.J. 1998) (citing *United States v. Kordel*, 397 U.S. 1, 12 n.27 (1970)).

15. "'[S]imultaneous criminal and civil cases involving the same or closely related facts may give rise to Fifth Amendment concerns sufficient to warrant a stay of the civil proceedings.'" *Sherrod v. Williams*, 2015 U.S. Dist. LEXIS 173352, *4 (S.D. Ohio – Dec. 31, 2015) (citing *Chao v. Fleming*, 498 F. Supp. 2d 1034, 1037 (W.D. Mich. 2007)).

16. "'Courts are afforded the discretion to grant a stay because the denial of a stay could impair a party's Fifth Amendment privilege against self-incrimination, extend criminal discovery beyond the limits set forth in Federal Rule of Criminal Procedure 16(b), expose the defense's theory to the prosecution in advance of trial, or otherwise prejudice the criminal case.'" *Chao*, 498 F. Supp. 2d at 1037 (citation omitted).

17. In the instant action, Boback initiated this lawsuit against LabMD, Daugherty, and Wallace, and subsequently, a criminal investigation was initiated by the FBI in relation to issues that overlap between this lawsuit and the FBI's investigation.

18. Accordingly, Boback seeks a temporary stay of this lawsuit, including with respect to LabMD's and Daugherty's attempt to depose Boback and their discovery requests served upon Boback, in order to allow for the FBI's criminal investigation to proceed unimpeded while Boback preserves his constitutional privileges.

19. There is precedent for a Pennsylvania court granting a stay in the situation where a plaintiff under criminal investigation files a lawsuit alleging that the defendant was liable for defamation. *See Spanier v. Freeh*, 95 A.3d 342, 344-45 (Pa. Super. Ct. 2014).

20. Furthermore, courts in Pennsylvania have utilized a six (6) factor analysis in determining whether a stay should be imposed in a civil lawsuit while a party is under criminal investigation. *Spanier*, 95 A.3d at 345; *Adelphia*, 2003 U.S. Dist. LEXIS 9736, at *7-8.

21. The six factors are:

> a. The extent to which the issues in the civil and criminal cases overlap;
> b. The status of the criminal proceedings, including whether any [parties] have been indicted;
> c. The [parties'] interests in expeditious civil proceedings weighed against the prejudice to the [parties] caused by the delay;
> d. The burden on the [non-moving party];
> e. The interests of the court; and,
> f. The public interest.

Adelphia, 2003 U.S. Dist. LEXIS 9736, at *7-8 (citing *Walsh Secs., supra*).

22. Application of the above six-factor analysis demonstrates that Boback's Motion for Stay should be granted.

23. With respect to the <u>first factor</u>, upon information and belief, the FBI's raid of Tiversa's offices concerns alleged false statements made to the Government, and these are the same issues that are present in the instant matter. *See generally* 2d Am. Compl.; Reuters Report (Ex. A).

24. Accordingly, the issues in the civil and criminal cases overlap.

25. With respect to the <u>second factor</u>, to the best of Boback's knowledge, the FBI's criminal investigation has not resulted in the filing of any Indictments.

26. However, a motion for stay is properly granted "even though an indictment or information has not yet been returned, if the Government is conducting an active parallel criminal investigation." *Walsh Secs.*, 7 F. Supp. 2d at 527-28 (noting that interrogatory and

deposition discovery posed a substantial risk of self-incrimination even where the Government's criminal investigation was at the pre-indictment stage).

27. Upon information and belief, the FBI's investigation is ongoing.

28. Accordingly, the FBI's investigation represents an active parallel criminal investigation weighing in favor of granting Boback's Motion to Stay.

29. With respect to the third factor, granting Boback's Motion to Stay will not unduly prejudice LabMD or Daugherty, as the requested stay is only for a temporary period of time.

30. Furthermore, any concern about an indefinite stay may be alleviated by allowing the parties to petition the Court to lift or modify the stay if there is a change in circumstances that warrant modification. *Walsh Secs.*, 7 F. Supp. 2d at 529.

31. With respect to the fourth factor, if a stay is not imposed, Boback must choose between waiving his Fifth Amendment rights and prosecuting his civil lawsuit against LabMD and Daugherty, or asserting the privilege and causing potentially fatal injury to his case. *Id.* at 528.

32. Furthermore, if Boback waives his constitutional privileges, there is a significant risk that he would expose a defense theory in advance of a potential criminal trial. *Chao*, 498 F. Supp. 2d at 1037 (citation omitted).

33. With respect to the fifth factor, absent a stay, "interrogatory and deposition discovery would likely cause inefficiency," as Boback will be forced to assert constitutional privileges, which will burden the Court with constantly having to decide privilege issues. *Walsh Secs.*, 7 F. Supp. 2d at 528.

34. Staying this matter until the conclusion of the criminal proceedings will eliminate the need for the Court to rule on privilege issues. *Adelphia*, 2003 U.S. Dist. LEXIS 9736, *15 (citing *Walsh Secs.*, 7 F. Supp. 2d at 528).

35. Finally, with respect to the sixth factor, imposing a stay in the instant matter will not be adverse to the public, unlike situations where civil cases are brought by governmental agencies to protect the public (e.g., halting the distribution of mislabeled drugs, preventing the dissemination of misleading information to the investing public). *Walsh Secs.*, 7 F. Supp. 2d at 529.

36. "In fact, a stay in this case would benefit the public by allowing the Government to conduct a complete, unimpeded investigation into potential criminal activity." *Id.*

37. Furthermore, the public has an interest in seeing that all citizens' constitutional privileges are protected.

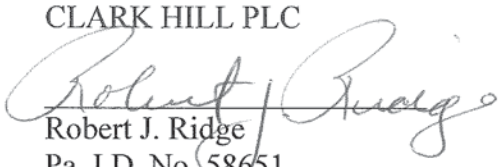
38. As demonstrated above, all six factors of the analysis as to whether to grant a motion for stay weigh in favor of granting Boback's Motion to Stay.

WHEREFORE, Plaintiff, Robert J. Boback, respectfully requests that this Honorable Court grant his Motion to Stay and enter the proposed Order attached hereto.

Respectfully submitted,

CLARK HILL PLC

Date: July 20, 2016



Robert J. Ridge
Pa. I.D. No. 58651
Brandon J. Verdream
Pa. I.D. No. 204162

EXHIBIT B

1

2 IN THE COURT OF COMMON PLEAS OF
ALLEGHENY COUNTY, PENNSYLVANIA

3

- - -

4

TIVERSA HOLDING CORP., and)CIVIL DIVISION
5 ROBERT J. BOBACK,)
)NO. GD 14-016497
6 Plaintiffs,)
)
7 v.)
)
8 LabMD, INC., MICHAEL J.)
DAUGHERTY, RICHARD EDWARD)
9 WALLACE and CAUSE OF ACTION)
INSTITUTE,)
10)
Defendants.)

11

- - -

12

MOTIONS HEARING

13

- - -

14

BEFORE HONORABLE CHRISTINE A. WARD

15

Thursday, August 25, 2016
16 10:25 a.m.

17

- - -

18 Whereupon the above-entitled matter came on for hearing before the HONORABLE CHRISTINE A. WARD, at
19 the City-County Building, Room 820, Pittsburgh, Pennsylvania, and the proceedings were as follows:

20

21 Reported by:
Sara A. Acklin
22 Court Reporter

23

- - -

24 **REPRODUCTION OF THIS TRANSCRIPT IS PROHIBITED BY ANY MEANS, ELECTRONIC, HARD COPY OR OTHERWISE WITHOUT
25 AUTHORIZATION FROM THE CERTIFYING AGENCY**

1

2 APPEARANCES:

3 For the Plaintiffs: Clark Hill, PLC
by Robert J. Ridge, Esq.
4 by Elizabeth F. Collura, Esq.

5

McGuireWoods, LLP
6 by Jarrod D. Shaw, Esq.

7 For the Defendants,
LabMD and Michael J.
8 Daugherty: Duane Morris, LLP
by Kenneth M. Argentieri, Esq.
9 by Cynthia Counts, Esq.

10 James W. Hawkins, LLC
by James W. Hawkins, Esq.
11

For the Defendant,
12 Richard Edward
Wallace: Bryan Cave, LLP
13 by Mary Beth Buchanan, Esq.

14

15

16

17

18

19

20

21

22

23

24

25

1 **August 25, 2016**
2 I think it will be difficult for anything to take --
3 everything does take more than ten to fifteen
4 minutes.
5 MS. COUNTS: I am willing to do it this
6 time. I am really.
7 THE COURT: Without further adieu,
8 Mr. Ridge, I think you are up on the Motion to Stay.
9 MR. RIDGE: Thank you, Your Honor.
10 Your Honor, we appeared before this Court,
11 as you know, on May 11, 2016, for the purpose of a
12 status conference, and at that time, I informed the
13 Court that it was my intention to review the book
14 written by Mr. Daugherty and some of the allegations
15 that were by Mr. Daugherty in the context of the
16 circumstances under which they were made for the
17 purpose of analyzing the viability of those claims
18 and whether there were any claims that I thought we
19 might not be pursuing now that Tiversa is out of the
20 case.
21 Less than 60 days after we reached an
22 agreement that I would be given 60 days at least to
23 review that book, I received a Notice of Deposition
24 and a set of Interrogatories and Request For
25 Production of Documents. I received that request

1 August 25, 2016
2 without any prior notice, without any request to meet
3 and confer, without any request about, hey, exactly
4 where you are in this case. And so regrettably, Your
5 Honor, I filed this Motion to Stay because it does
6 seem to me that the only way I can be assured of
7 relief is not through agreement with counsel, but by
8 some Order of the Court.
9 Having said that, Your Honor, the basis for
10 the Motion to Stay is that the Court knows the
11 existence of parallel civil and criminal
12 investigations involving, essentially, the same
13 allegations. In the -- we are aware of a criminal
14 investigation and became aware of a criminal
15 investigation by virtue of the execution of the
16 search warrant at Tiversa properties on March 1 of
17 2016.
18 When I looked at the case law regarding
19 staying civil proceedings in lieu of civil
20 proceedings, I identified, like everyone else has in
21 this case, the six factor test that can be traced
22 back to In Re: Adelphia Communications and the prior
23 cases in that line of cases.
24 And if circumstance factors, Your Honor, are
25 things that I will use as a mechanism to sort of

1 **August 25, 2016**
2 bring us to where we are right now.
3 The first issue is whether there is overlap
4 between the criminal investigation and the civil
5 case. As the Court knows, this civil case is a
6 defamation case regarding the question of whether
7 Mr. Daugherty's statements defame Mr. Boback. It was
8 originally a question of whether Mr. Daugherty's
9 statements defamed Mr. Boback and Tiversa, but
10 Tiversa has since withdrawn its claim.
11 In order to understand what exactly --
12 whether this is overlap between the two, I made
13 arrangements with and did go and visit with the
14 prosecutor who is handling the investigation in
15 Washington, D.C. on August 10, 2016. The prosecutor
16 advised me that, while he wasn't at liberty to say
17 much because it's a pending investigation, he would
18 tell me that they are in the early stages of the
19 investigation and there is a considerable amount of
20 electronic data that they downloaded in pursuit -- in
21 the execution of the search warrant.
22 And, again, he was not at liberty to tell me
23 much, but what he would tell me is that the focus of
24 their investigation has to do with communication to
25 the government, whether it's the FTC or the United

1 States Congress.
2 With that in mind, Your Honor, I took a look
3 at the request that are -- that have been propounded
4 here, and those requests touch on exactly the same
5 subject matters identified -- and I will give the
6 Court the benefit of my review -- it is at the LabMD
7 and Michael Daugherty's First Set of Interrogatories
8 and Request For Production Documents directed to
9 Robert Boback, No. 6, identify all persons with whom
10 Mr. Boback has had communications relating to the
11 17/18 file.
12 By the way, Your Honor, one other thing I
13 wanted to mention so we are on the same page, when we
14 had the agreement that I would review the file, the
15 conclusion of my review was to be if I wasn't going
16 to abandon all of the allegations, that I would
17 confer with counsel and try to come up with a case
18 management plan that the Court could accept.
19 We have not been given that opportunity,
20 Your Honor, and that is why I am in agreement with
21 your request for a case management plan in connection
22 with this hearing today. But let me first tell you
23 what the overlap is.
24 No. 6, identify all persons with whom Mr.
25

1 **August 25, 2016**
2 Boback has had communications relating to the 17/18
3 file.
4 No. 7, identify all communications that Mr.
5 Boback has had relating to the 17/18 file.
6 No. 8, identify the various IP addresses
7 from which the 17/18 file was downloaded by Tiversa
8 as alleged in Paragraph 16 of the Complaint.
9 No. 9, identify the Tiversa employee who
10 downloaded the 17/18 file.
11 No. 10, identify the owners of various IP
12 addresses identified in the Answer to Interrogatory
13 8.
14 No. 11, identify the owners of all IP
15 addresses referenced in the April 18, 2008, Tiversa
16 investigation request form.
17 No. 12, state the basis for why the IP
18 addresses referenced in the April 18, 2008, Tiversa
19 investigation request form and incident record form.
20 The August 12, 2008, Tiversa forensic investigation
21 report and the Tiversa forensic investigation report
22 is attached as Exhibit 10 to Defendant's appendix for
23 the Motion for Sanctions. I am really not sure what
24 that one means.
25 No. 13, identify all persons at the Federal

1 **August 25, 2016**
2 Trade Commission with whom you communicated.
3 No. 14, identify all communications that you
4 had with any individual at the FTC regarding LabMD or
5 peer-to-peer networks.
6 So in essence, Your Honor, the subject
7 matter of the discovery in this case is, essentially,
8 the communications that LabMD -- I am sorry, that
9 Tiversa and Mr. Boback have had with the government,
10 including the FTC and the United States Congress.
11 So the question of overlap, it seems to me,
12 is fairly clear. While I can't tell you that anyone
13 has been indicted in this case -- because the second
14 factor to be consider under the In Re: Adelphia
15 Communication standard is what's the status of the
16 criminal investigation -- while I can't tell you that
17 anyone has been indicted in this case, I can tell you
18 that Mr. Boback, for the most part, is the conduit of
19 all of that information. He may not be the source,
20 but he is the conduit of all of that information or
21 the vast majority of that information to the United
22 States Government.
23 So that having been the case, it does seem
24 to me that it is a fair assumption that Mr. Boback
25 will be involved at some level in the government's

1 **August 25, 2016**
2 criminal investigation should it proceed.
3 The third issue that the Adelphia case
4 raises is, what are the interest and expeditious
5 resolution of the civil proceedings weighed against
6 the prejudice by delay. And in that context, Your
7 Honor, I think it's important that the Court
8 understand that sometime either in late July or early
9 August the FTC issued its opinion which reversed the
10 Administrative Law Judge and found that LabMD had, in
11 fact, violated its standards on privacy.
12 Now, the FTC opinion is relevant in this
13 case for a couple of different reasons, but the most
14 important is this. At Page 31 of the FTC's opinion,
15 the commission holds that, first, the record does not
16 show that Tiversa, whatever its motives, unlawfully
17 obtained the 17/18 file. LabMD made the file freely
18 available for public viewing through LimeWire.
19 That, Your Honor, that finding by the FTC
20 has to be reviewed as it relates to this case in the
21 context of the allegations in the Complaint that
22 relate to theft. In particular, Your Honor, I am
23 referring to the allegations at Paragraph No. 33 in
24 which Mr. Boback has alleged that Mr. Daugherty's
25 book describes the party's interactions as a theft

1 **August 25, 2016**
2 That is not an issue we really want to discuss, Your
3 Honor. I don't doubt that the Fifth Amendment can be
4 waived so long as there is an immediate sort of
5 reasonable apprehension that you could be prosecuted,
6 you would waive it. That is not what happened here.
7 And Griffin, Your Honor, is an ancient case,
8 1964 I think is the date on the case. And in that
9 case, the real issue is whether the prosecutor --
10 that is how old this is -- whether the prosecutor
11 could comment on the Defendant's refusal to testify
12 or respond. So I doubt that that case, Your Honor,
13 has any real bearing on the outcome here.
14 In the final analysis, Your Honor, I think
15 the amount of stay that we've requested is
16 reasonable. I think the overlap between this
17 investigation and the criminal investigation is
18 obvious. And I think in order to protect Mr.
19 Boback's Fifth Amendment rights, the stay should be
20 enforced, at least as it relates to him, because he
21 is, quite clearly, going to be someone to whom the
22 United States will have to pay attention if that
23 continues to be the focus of the criminal
24 investigation.
25 That is all I have, Your Honor, unless you

EXHIBIT 19

In the Matter of:

LabMD, Inc.

May 15, 2014
Final Prehearing Conference

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

9

1 JUDGE CHAPPELL: I'd love hearing him
2 questioned, but --
3 MR. SHERMAN: We don't find his testimony to be
4 necessary.
5 JUDGE CHAPPELL: Okay. Thank you.
6 As a former prosecutor, I just have to comment
7 on things like that.
8 All right. So now we're down to respondent's
9 objections to complaint counsel witnesses. I've got a
10 couple objections, one as to the designated testimony of
11 Curt --
12 MR. SHERMAN: Kaloustian.
13 JUDGE CHAPPELL: -- Kaloustian -- thank you --
14 the nonpublic hearing taken in the Phase II
15 investigation of LabMD, otherwise known here as an
16 investigational hearing transcript or IHT.
17 The rule has been changed recently, 3.43(b), and
18 IHTs are now admissible. I'm not saying I agree with
19 that, but that's the rule.
20 Respondent also objects to complaint counsel's
21 expert witness Professor Hill's heavy reliance on
22 Mr. Kaloustian's uncross-examined testimony.
23 Again, IHT testimony is admissible, but be
24 advised that -- first of all, your objection goes to
25 the weight, not the admissibility, so I'm going to

10

1 overrule that objection. But the parties are advised
2 that although they are admissible, they're taken
3 without counsel, without respondent present, don't
4 expect them to be given a lot of weight in this
5 proceeding.
6 When they are cited in posttrial findings, the
7 opposing side is encouraged to point out in their
8 responses that it was taken from an IHT.
9 Let me talk about motions to quash.
10 Two nonparties have filed motions to quash the
11 trial subpoenas served on them by respondent,
12 Eric Johnson --
13 (Pause in the proceedings.)
14 JUDGE CHAPPELL: And the second is
15 Robert Boback.
16 MR. SHERMAN: "Boback."
17 JUDGE CHAPPELL: "Boback."
18 Their objections seem to be based on scheduling
19 issues and rely principally on the fact that they
20 already testified by deposition and shouldn't be
21 required to come here live.
22 I've got respondent's opposition to
23 Eric Johnson's motion.
24 Does complaint counsel intend to file a response
25 or do you want to address that motion now?

11

1 MS. VANDRUFF: Thank you, Your Honor.
2 Complaint counsel does not intend to take a
3 position as to either motion, although we would just
4 note that while we had listed Mr. Boback as a potential
5 live witness, we're satisfied with having submitted to
6 the court his deposition testimony.
7 Likewise, as indicated in Mr. Boback's motion,
8 we have also consented to the alternative relief that
9 Mr. Boback requested, which is that he appear by
10 videoconference.
11 JUDGE CHAPPELL: Did you mean to be talking
12 about Boback the whole time there, because you said
13 likewise Mr. Boback?
14 MS. VANDRUFF: Yes, Your Honor.
15 JUDGE CHAPPELL: You're not addressing
16 Eric Johnson.
17 MS. VANDRUFF: With respect to Mr. Johnson,
18 complaint counsel is not taking a position.
19 JUDGE CHAPPELL: No position at all. But with
20 Boback, you're not intending to call him live.
21 MS. VANDRUFF: We are not taking a position with
22 respect to the motion and we are not intending to call
23 him live. That's correct, Your Honor.
24 JUDGE CHAPPELL: Okay. Which takes care of the
25 subpoena, if possible.

12

1 Does that change your position if he's not going
2 to be called live?
3 MR. SHERMAN: No, it doesn't, Your Honor.
4 JUDGE CHAPPELL: You still want him here.
5 MR. SHERMAN: We want him here. We believe that
6 it is of significant benefit to the trier of fact to
7 have the witness here to be observed as he testifies for
8 all the benefits of live interaction between humans, as
9 the judge is well aware.
10 JUDGE CHAPPELL: I'm going to take this under
11 advisement. I'll rule on this motion later -- actually
12 two motions later.
13 Well, let me talk about --
14 MR. SHERMAN: Oh, Your Honor, may I?
15 JUDGE CHAPPELL: Yeah. Actually I've got your
16 response on Johnson but not on Boback.
17 Do you intend to file a written response?
18 MR. SHERMAN: Today.
19 JUDGE CHAPPELL: Good. Then I'll hold off until
20 I get your response.
21 MR. SHERMAN: Thank you, Your Honor.
22 JUDGE CHAPPELL: All right. I'll ask my staff
23 to make note of that.
24 All right. Let's talk about exhibits and
25 objections thereto.

41

1 So hopefully this is clear. If you want to use
2 any deposition testimony in this case in your posttrial
3 briefing to support any point or cause, submit the
4 entire transcript. How's that?
5 MS. VANDRUFF: Thank you, Your Honor.
6 MR. SHERMAN: That's good, Your Honor.
7 And just for clarity, complaint counsel served
8 us late last night with specific objections to our
9 deposition designations, and I -- in my mind, what you
10 just said, your ruling here makes those moot.
11 JUDGE CHAPPELL: Yes. I have found over time
12 that the way I just described it some moments ago is the
13 best way to deal with this, because I could sit here and
14 rule on these objections for days, but a lot of them are
15 going away anyway by the time this is done. When we get
16 to that final briefing, you're looking at the trial
17 transcript, and a lot of it goes away. That's why it's
18 more efficient just to wait and deal with it in a
19 posttrial brief.
20 And nobody is harmed there, nobody is
21 prejudiced, because everybody knows what we're doing.
22 It's out in the open.
23 Any objection to me doing it that way?
24 MR. SHERMAN: Absolutely not.
25 MS. VANDRUFF: No, Your Honor. Thank you.

42

1 JUDGE CHAPPELL: Let's talk about in camera
2 issues.
3 I don't know if you noticed when you walked in,
4 we've got a sign out there. And when the parties
5 request it, we'll go into in camera session, and then
6 I'll remove everyone from the courtroom who's not
7 subject to the protective order. And we have a sign we
8 will turn to keep people from wandering in.
9 And our bailiff Ironsides, he is the enforcer.
10 Ironsides will make sure no one comes in who's not
11 supposed to be here during an in camera session.
12 I saw three joint motions for in camera
13 treatment. By orders dated May 6, 2014, permanent
14 in camera treatment was granted to exhibits
15 containing sensitive personal information and also
16 in camera treatment for a period of six years to the
17 fraud survey questions of Mr. Van Dyke and
18 Javelin Strategy & Research.
19 On May 14, I saw an additional motion for
20 in camera treatment seeking permanent in camera
21 treatment for one exhibit containing sensitive personal
22 information. I'm going to grant that motion, and an
23 order will issue shortly regarding that.
24 MS. VANDRUFF: Thank you, Your Honor.
25 JUDGE CHAPPELL: Let's talk about how we're

43

1 going to proceed in here with in camera information if
2 you haven't been here before.
3 You're instructed to be aware of the documents
4 and any information derived from those documents that
5 have been granted in camera treatment. If you wish to
6 question a witness about that document or that
7 information, you need to ask me, you need to request to
8 move into an in camera session. At that point I will
9 clear the courtroom of persons who are not authorized to
10 be in here.
11 And in keeping with the least amount of
12 disruption possible, you shall segregate your
13 questioning, your examining of witnesses, so that any
14 section on in camera materials is grouped together so
15 that I'm not clearing the courtroom and bringing people
16 back in more than necessary.
17 I have found that the best way to do this,
18 whoever calls the witness reserves in camera issues
19 until the end of their examination, and then the person
20 conducting cross-exam conducts their in camera portion
21 of questioning at the beginning of their examination.
22 In addition, counsel shall instruct witnesses to
23 ensure they do not disclose in camera testimony in open
24 session. We really don't want anything bleated out by a
25 witness who may or may not know what's in camera.

44

1 Any questions on how we're going to handle
2 in camera info?
3 MS. VANDRUFF: No, Your Honor.
4 MR. SHERMAN: No, Your Honor.
5 JUDGE CHAPPELL: Ironsides, can you come up when
6 you get a minute.
7 I have a pending motion filed by respondent on
8 May 2, 2014 seeking to limit the relevant time period
9 concerning adequacy of respondent's data security
10 practices.
11 Now, it may appear that I'm reading to you, but
12 I'm going to make a bench ruling, so I am going to be
13 reading from my script here.
14 So the motion involves adequacy of respondent's
15 data security practices to the time period analyzed by
16 Dr. Raquel Hill, complaint counsel's proffered expert,
17 which is January 2005 to July of 2010.
18 Respondent is questioning what is the relevant
19 time period and seeks not only to limit Dr. Hill's
20 testimony to this time period, 2005 to 2010, but also to
21 exclude any other witness from the FTC from providing
22 evidence concerning adequacy of LabMD's security
23 practices after July 2010.
24 Complaint counsel filed an opposition on May 13,
25 2014 and acknowledged Dr. Hill's report and her opinions

45

1 are limited to the time period January 2005 through
2 July 2010, and complaint counsel agrees it will not
3 elicit testimony from Dr. Hill outside of that time
4 frame.
5 However, complaint counsel argues, simply
6 because Dr. Hill's opinion is limited does not mean
7 complaint counsel is precluded from presenting other
8 evidence concerning the adequacy of respondent's data
9 after July 2010.
10 Complaint counsel also argues that evidence of
11 the data security practices after July 2010 and through
12 the end of discovery remains relevant to the
13 allegations in the complaint and the proposed
14 injunctive remedy.
15 Complaint counsel also notes that the motion is
16 untimely because respondent failed to file by
17 April 22, 2014, the deadline for motions in limine
18 covered by the scheduling order.
19 I've reviewed the parties' filings and fully
20 considered the issue. This is my ruling.
21 Respondent's motion is untimely under the
22 scheduling order, and there appears to be no
23 justification for the failure to file it before the
24 deadline, given that the expert report was served on or
25 about March 18, 2014. However, that's not why I'm going

46

1 to overrule your motion or deny your motion.
2 Respondent has failed to demonstrate that
3 evidence of respondent's data security practices during
4 the time period after July 2010 and through the end of
5 discovery is not relevant and clearly inadmissible for
6 all purposes, which is our motion in limine standard.
7 At a minimum, this later time period is relevant to the
8 proposed relief in this case.
9 Accordingly, respondent's motion to limit
10 evidence to the time frame of complaint counsel's expert
11 report is denied.
12 However, Dr. Hill's testimony is limited to the
13 opinions expressed in her report and thus to the time
14 period January 2005 through July 2010.
15 Any questions?
16 MR. SHERMAN: None whatsoever, Your Honor.
17 MS. VANDRUFF: No, Your Honor. Thank you.
18 JUDGE CHAPPELL: Let's talk about trial timing.
19 Pursuant to rule 3.41(b), this hearing is
20 limited to no more than 210 hours. Assuming
21 six-and-a-half-hour days, which generally we have after
22 our breaks are taken out, this equates to about 32 total
23 days of trial.
24 Under that same rule, 3.41(b)(4), each side is
25 allotted no more than half of the time. That's about

47

1 16 days each.
2 As I instructed the parties at the initial
3 conference, the parties are charged with keeping track
4 of the time allotted.
5 Have you developed a system?
6 MR. SHERMAN: I have not, Your Honor. But we
7 will do so prior to the beginning of the hearing.
8 MS. VANDRUFF: Correct, Your Honor. We will
9 work with respondent's counsel to do that.
10 JUDGE CHAPPELL: And it's not required if you
11 are absolutely sure we will come under the wire and not
12 need the full amount of time, which I would encourage if
13 possible.
14 Let's talk about trial dates.
15 Because we all have numerous other matters to
16 attend to, we generally will be in court four days a
17 week. Normally that's going to be a Monday or Friday
18 out of court to better accommodate those from out of
19 town.
20 I have the following dates that I'm blocking as
21 of today:
22 May 26, which is a holiday.
23 June 2.
24 June 9.
25 June 16.

48

1 June 23.
2 Those are all Mondays. If we are still in trial
3 beyond those dates, we will revisit scheduling. And I
4 can tell you, if we're still here in July, which I hope
5 we're not, we also will not be here July 14.
6 Do the parties have any particular dates you
7 need to line out that you're aware of today?
8 Let's start with respondent.
9 MR. SHERMAN: I am not aware of them today. Is
10 it possible, however, Your Honor, that we could be given
11 an opportunity to check on dates and submit that to the
12 court -- I don't know how many --
13 JUDGE CHAPPELL: How long do you need?
14 I mean, is this today or is this --
15 MR. SHERMAN: Oh, absolutely, I can do it by the
16 end of the day. But --
17 JUDGE CHAPPELL: I generally am not going to put
18 this in a written motion.
19 MR. SHERMAN: I want to stay married.
20 JUDGE CHAPPELL: That's a worthy goal, so...
21 Are you aware of any dates you think you need
22 off?
23 MS. VANDRUFF: Given the schedule that
24 Your Honor just described, then no, Your Honor, we don't
25 anticipate there being any issues on our side.

EXHIBIT 20

PUBLIC

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

DOCKET NO. 9357

In the Matter of

LabMD INC.,
a corporation

Respondent.

INITIAL DECISION

D. Michael Chappell
Chief Administrative Law Judge

Date: November 13, 2015

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. SUMMARY OF COMPLAINT AND ANSWER 1
  - 1. The Complaint 1
  - 2. Respondent's Answer and Defenses 2
- B. PROCEDURAL HISTORY 5
  - 1. Overview 5
  - 2. Procedural Summary 6
- C. EVIDENCE 11
- D. SUMMARY OF INITIAL DECISION 13

II. FINDINGS OF FACT 15
- A. KEY TERMS 15
- B. TESTIFYING EXPERTS 15
  - 1. Complaint Counsel's Experts 15
    - a. Dr. Raquel Hill 15
    - b. Mr. Rick Kam 16
    - c. Mr. James Van Dyke 16
    - d. Dr. Clay Shields 17
  - 2. Respondent's Expert 17
    - a. Mr. Adam Fisk 17
- C. RESPONDENT 18
  - 1. Background Information 18
  - 2. Collection of Personal Information in Connection with Lab Testing 20
  - 3. Insurance Aging Reports 21
  - 4. Collection of Personal Information in Connection with Payments 22
- D. THE 1718 FILE INCIDENT 22
  - 1. Peer-to-Peer Networks 22
  - 2. The 1718 File 24
    - a. Background facts 24
    - b. LabMD discovery 25
  - 3. Tiversa 26
    - a. Tiversa's business 26
    - b. Tiversa's dealings with LabMD 29
    - c. Tiversa's role as source for FTC investigation 30
    - d. CX0019 32
  - 4. Credibility Findings Concerning the 1718 File Incident 33
  - 5. Professor Eric Johnson 34
- E. THE SACRAMENTO INCIDENT 36
  - 1. Sacramento Police Department's Discovery of LabMD Documents 36
  - 2. Connection between the Sacramento Documents and LabMD's Computer Network 37
  - 3. Follow up to Discovery of the Sacramento Documents 39
  - 4. Lack of Foundation for Admission of CX0451 39
- F. IDENTITY THEFT HARM 41

III. ANALYSIS 45
A. BURDEN OF PROOF 45
B. JURISDICTION 46
C. LEGAL FRAMEWORK FOR DETERMINING UNFAIR CONDUCT 47
D. CONSUMER HARM ANALYSIS 49
1. Terminology 49
2. Overview of Arguments on Substantial Consumer Injury 50
3. Actual or Likely Harm 52
4. Complaint Counsel's Proffered Consumer Injury Experts 56
5. The 1718 File Incident 57
a. Summary of facts 57
b. Overview of analysis 59
c. Identity theft harm 60
i. Mr. Rick Kam 60
ii. Mr. James Van Dyke 62
d. Medical identity theft harm 66
e. Reputational and other harms 68
f. Conclusion 69
6. The Sacramento Incident 70
a. Summary of facts 70
b. Summary of arguments 71
c. Connection to LabMD's computer network 72
d. Identity theft harm 75
i. Mr. Rick Kam 75
(a) Opinions 75
(b) Exclusion of CX0451 76
ii. Mr. James Van Dyke 79
e. Conclusion 80
7. Risk of Harm to Consumers whose Personal Information is Maintained on LabMD's Computer Network 80
a. Introduction 80
b. Analysis 82
c. Conclusion 87
E. CONCLUSION 87

IV. SUMMARY OF CONCLUSIONS OF LAW 89

ORDER 92

I. INTRODUCTION

A. SUMMARY OF COMPLAINT AND ANSWER

1. The Complaint

The Administrative Complaint in this case ("Complaint"), issued by the Federal Trade Commission ("FTC" or "Commission") on August 28, 2013, charges that Respondent LabMD, Inc. ("Respondent" or "LabMD"), a clinical testing laboratory, failed to provide "reasonable and appropriate" security for personal information maintained on LabMD's computer networks, and that this conduct "caused or is likely to cause" substantial consumer injury. Therefore, the Complaint alleges, Respondent is liable for "unfair" acts or practices under Section 5(a) of the Federal Trade Commission Act ("FTC Act"). Complaint ¶¶ 10, 17-21, 22-23.

Specifically, the Complaint alleges that "[R]espondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." Complaint ¶ 10. "Among other things," according to the Complaint, Respondent:

(a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information;
(b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks;
(c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
(d) did not adequately train employees to safeguard personal information;
(e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures;
(f) did not maintain and update operating systems of computers and other devices on its networks; and
(g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks.

Complaint ¶ 10(a)-(g).

The Complaint alleges two "security incidents" occasioned by Respondent's alleged unreasonable data security. The first incident, according to the Complaint, occurred in May 2008, when a "third party" informed Respondent that a June 2007 insurance aging report was "available" on a peer-to-peer ("P2P") file-sharing network, through a file-sharing application

called LimeWire. Complaint ¶ 17. The insurance aging report allegedly contained personal information, such as names, dates of birth, Social Security numbers ("SSNs"), current procedural terminology ("CPT") codes, and health insurance company names, addresses, and policy numbers, for approximately 9,300 patients of LabMD's physician clients. Complaint ¶ 19. This insurance aging report, consisting of 1,718 pages, is referred to herein as the "1718 File."

For the second alleged security incident asserted to have been caused by Respondent's alleged failure to protect data on its computer networks, the Complaint alleges that in October 2012, "more than 35 Day Sheets" and "a small number of copied checks" were found in the possession of individuals who subsequently pleaded "no contest" to identity theft charges (the "Sacramento Documents"). Complaint ¶ 21. The Complaint further claims that the Sacramento Documents included personal information such as names and Social Security numbers, and that some of the Social Security numbers have been used by people with different names, which the Complaint alleges indicates use of Social Security numbers by identity thieves. Complaint ¶ 21.

The Complaint concludes that Respondent's alleged failure to employ "reasonable and appropriate" measures to prevent unauthorized access to personal data caused, or is likely to cause, substantial harm to consumers that is not reasonably avoidable by consumers or outweighed by benefits to consumers or competition, and therefore constitutes an unfair practice under Section 5 of the FTC Act. Complaint ¶¶ 22, 23.

2. Respondent's Answer and Defenses

Respondent filed its Answer and Defenses to the Complaint on September 17, 2013. By Order issued July 27, 2015, Respondent was granted leave to add an additional affirmative defense, and Respondent filed its First Amended Answer and Defenses on July 31, 2015 ("Amended Answer"). The Amended Answer denies all material allegations of the Complaint, except as noted below.

Respondent's Amended Answer admits that it is a Georgia corporation, and further states that it is a clinical laboratory that conducts tests on specimen samples and reports the test results to authorized physicians. Amended Answer ¶¶ 1, 3. Respondent further admits that it files insurance claims for the testing charges with health insurers. Amended Answer ¶ 4. In

connection with the foregoing activities, Respondent receives patient names, addresses, dates of birth, gender, telephone numbers, Social Security numbers, lab tests and lab testing codes, and health insurance company names and policy numbers. Amended Answer ¶ 6. Respondent further admits that it uses a computer network in its business to file insurance claims and prepare bills, and that it creates spreadsheets that may include patient information and insurance information. Amended Answer ¶ 9.

With respect to the alleged security incidents set forth in the Complaint, Respondent's Amended Answer states that Tiversa Holding Company ("Tiversa") contacted LabMD in May 2008 claiming to have obtained the 1718 File through LimeWire. Amended Answer ¶ 17. Respondent further states its belief that LimeWire had been downloaded and may have been installed on a computer used by LabMD's billing department manager "no later than" 2006. Amended Answer ¶ 18.

The Amended Answer includes six defenses, including: the Complaint fails to state a valid claim; the Commission lacks subject matter jurisdiction over the claims made in this case; the Commission lacks statutory authority to regulate the acts and practices alleged in the Complaint, making the Commission's actions unlawful; the alleged acts and practices have not caused, and are not likely to cause, substantial injury that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition; the enforcement action against Respondent violates Respondent's due process rights because the Commission has not provided fair notice of the data security standards that the Commission believes Section 5 prohibits or requires; and, the claims alleged in the Complaint are barred by Article II of the United States Constitution because the presiding Administrative Law Judge ("ALJ") is an "inferior officer" that has not been properly appointed by the Commissioners of the FTC, the President, or the Judiciary (the "Appointments Clause" defense). Amended Answer at 5-6.

Respondent presented each of the foregoing defenses, other than the Appointments Clause defense, in a pre-trial Motion to Dismiss filed November 12, 2013. Under the

Commission's Rules of Practice, the Motion was decided by the Commission[1] – the same entity that, when issuing the Complaint, stated it had "reason to believe" that LabMD violated the provisions of the FTC Act. Complaint at 1. The Commission rejected Respondent's defenses, holding that the statutory prohibition against unfair trade practices in Section 5 could be applied to allegedly unreasonable and injurious data security practices, and declined to dismiss the Complaint. *In re LabMD, Inc.*, 2014 FTC LEXIS 2 (Jan. 16, 2014) ("Commission Order on Motion to Dismiss").

In addition, Respondent filed a pre-trial Motion for Summary Decision on April 21, 2014, which, like Respondent's pre-trial Motion to Dismiss, was also decided by the Commission, pursuant to the Commission's 2009 Rule changes. *See* footnote 1. The Commission denied Respondent's Motion for Summary Decision, holding that there were genuine disputes about some of the factual issues raised by LabMD and that LabMD's liability "for engaging in 'unfair acts or practices' in violation of . . . 15 U.S.C. § 45(a) . . . must be resolved based on factual evidence presented at an evidentiary hearing." *In re LabMD, Inc.*, 2014 FTC LEXIS 126, at *1-2 (May 19, 2014).[2]

[1] The Commission amended Rule 3.22 of its Rules of Practice in 2009 to allow "the Commission to decide legal questions and articulate applicable law when the parties raise purely legal issues." Proposed rule amendments; request for public comment, 73 Fed. Reg. 58,832, 58,836 (Oct. 7, 2008). "[C]ommenters (including the [Section of Antitrust Law of the American Bar Association ('Section')], criticized the [Commission's] proposed Rule change as unfairly invading the province of the independent ALJ and compromising the Commission's dual roles as prosecutor and adjudicator." Interim final rules with request for comment, 74 Fed. Reg. 1804, 1809 (Jan. 13, 2009). "For example, the Section argued that the proposed changes . . . could raise concerns about the impartiality and fairness of the Part 3 proceeding by permitting the Commission to adjudicate dispositive issues, including motions to dismiss challenging the facial sufficiency of a complaint, shortly after the Commission has voted out the complaint finding that it has 'reason to believe' there was a law violation, without the benefit of an opinion by an independent ALJ." *Id.* A joint comment from former FTC Chairman Robert Pitofsky and Michael N. Sohn "similarly argued that the proposed rules, including Rule 3.22, would arguably infringe on the fairness of the Part 3 proceeding if the Commission more frequently 'invades what has heretofore been the province of an independent ALJ.'" *Id.* Dismissing these objections, the Commission amended its Rules of Practice to give to itself the authority to decide "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision[.]" 16 C.F.R. § 3.22(a).

[2] On December 17, 2013, Respondent filed a Motion to Disqualify Commissioner Brill from participating in this administrative proceeding, arguing that, based on her comments in two public speeches, Commissioner Brill had prejudged the facts of this case. Commissioner Brill issued a statement denying that she had prejudged the case, but concluding nevertheless that, to avoid an undue distraction from the issues raised in the Commission's Complaint against LabMD, she would recuse herself from further participation in the matter. *In re LabMD, Inc.*, 2013 FTC LEXIS 138 (Dec. 24, 2013). Respondent also filed two motions seeking to disqualify Commission Chairwoman Ramirez from participating further in this matter. By Orders dated June 15, 2015 and August 14, 2015, the Commission denied those motions. *In re LabMD, Inc.*, 2015 FTC LEXIS 142 (June 15, 2015); *In re LabMD, Inc.*, 2015 FTC LEXIS 185 (Aug. 14, 2015).

Further, concurrent with its Motion to File an Amended Answer to add the Appointments Clause defense, Respondent filed a Motion to Dismiss based on the Appointments Clause defense, the resolution of which the Administrative Law Judge had, on the record, deferred to the Initial Decision. Tr. 1492-1493, 1497-1502. The Commission, exercising its "plenary authority over this adjudication," denied Respondent's Motion to Dismiss based on the Appointments Clause defense, holding "that the Appointments Clause does not apply to the hiring of Commission administrative law judges." However, in order to "put[] to rest any possible claim that this administrative proceeding violates the Appointments Clause," the Commission "ratified Judge Chappell's appointment as a Federal Trade Commission administrative law judge and as the Commission's Chief Administrative Law Judge." *In re LabMD, Inc.*, 2015 FTC LEXIS 215, at *4-6 (Sept. 14, 2015) and Exhibit A thereto (FTC Minute dated September 11, 2015).

B. PROCEDURAL HISTORY

1. Overview

The evidentiary hearing began on May 20, 2014. FTC Complaint Counsel ("Complaint Counsel") rested its case on May 23, 2014. As more fully described below, completion of Respondent's case was delayed by proceedings to obtain prosecutorial immunity for a defense witness, and the case was reconvened on May 5, 2015. After completion of Respondent's witnesses and resolution of certain evidentiary motions,[3] the evidentiary hearing was completed on July 15, 2015. The hearing record was closed by Order dated July 20, 2015.[4]

Rule 3.51(a) of the Commission's Rules of Practice states that "[t]he Administrative Law Judge shall file an initial decision within 70 days after the filing of the last filed initial or reply proposed findings of fact, conclusions of law and order . . . ." 16 C.F.R. § 3.51(a). The parties filed concurrent post-trial briefs and proposed findings of fact on August 10, 2015. The parties filed replies to the other's proposed findings of fact and post-trial briefs on September 4, 2015.

[3] *See In re LabMD, Inc.*, 2015 FTC LEXIS 175 (July 15, 2015); *In re LabMD, Inc.*, 2015 FTC LEXIS 154 (June 22, 2015).

[4] Over 1,080 exhibits were admitted into evidence, 39 witnesses testified, either live or by deposition, and there are 1,504 pages of trial transcript. The parties' proposed findings of fact and conclusions of law, post-trial briefs, replies to proposed findings of fact and conclusions of law, and reply briefs total 2,066 pages.

Pursuant to Commission Rule 3.41(b)(6), closing arguments were held on September 16, 2015. Seventy days from the last filed reply proposed findings and conclusions of law and reply briefs is November 16, 2015.

2. Procedural Summary

Proceedings in this matter have been lengthy, with over 200 entries on the docket, including, among other filings, numerous discovery motions, sanctions motions, and motions to dismiss filed before and after commencement of the evidentiary hearing.[5] A detailed history is available on the FTC's website at https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter, and in the interest of brevity will not be repeated here. Instead, the following procedural summary focuses on certain events in the evolution of the case that have led to the unusual result of Complaint Counsel retreating from its own evidence – evidence upon which it had relied in substantial part to support its claim of consumer injury in this case – as explained below.

By way of background, the FTC commenced its investigation into LabMD's data security practices in 2010, based upon Tiversa's claim that the 1718 File, containing personal information, had been disclosed by means of a peer-to-peer file-sharing network. *See* Fed. Trade Comm'n, "Widespread Data Breaches uncovered by FTC Probe" (Feb. 22, 2010), *at* https://www.ftc.gov/news-events/press-releases/2010/widespread-data-breaches-uncovered-ftc-probe; *see also* Letter from Commissioner Brill Denying Motion to Limit or Quash Civil Investigative Demand, April 20, 2012 at 2, *at* https://www.ftc.gov/sites/ default/files/ documents/petitions-quash/labmd-inc./102-3099-lab-md-letter-ruling-04202012.pdf. Dissenting from the above-cited letter by Commissioner Brill denying Respondent's Motion to Quash or Limit Civil Investigative Demand, then-Commissioner Rosch warned against relying on information provided by Tiversa, stating that "Tiversa is more than an ordinary witness, informant, or 'whistle-blower.' It is a commercial entity that has a financial interest in

[5] At the conclusion of evidence presented by Complaint Counsel, Respondent moved to dismiss the Complaint for failure of Complaint Counsel's evidence to establish a *prima facie* case of unfair trade practices. By Order issued after the close of the record on July 21, 2015, Respondent's motion was denied. *In re LabMD, Inc.*, 2015 FTC LEXIS 182 (July 21, 2015). On April 24, 2015, Respondent filed another motion to dismiss, arguing that Complaint Counsel engaged in "misconduct and indiscretions" in the investigation and prosecution of this case, including with respect to its reliance on evidence provided by Tiversa, a motion which was also denied as premature. *In re LabMD, Inc.*, 2015 FTC LEXIS 122 (May 26, 2015).

intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." Dissenting Statement of Commissioner J. Thomas Rosch re FTC File No. 1023099 (June 21, 2012) at 1, *at* https://www.ftc.gov/sites/default/files/documents/ petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf. Former Commissioner Rosch further noted that, according to LabMD, after Tiversa's discovery of the 1718 File on a peer-to-peer network in 2008, Tiversa "repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD." *Id.* at 1-2. Former Commissioner Rosch advised that, under these circumstances, the FTC staff should not inquire about the 1718 File, and should not rely on Tiversa for evidence or information, in order to avoid the appearance of impropriety. *Id.*

FTC staff did not heed then-Commissioner Rosch's warning, and also did not follow his advice. Instead, Complaint Counsel chose to further commit to and increase its reliance on Tiversa. During discovery, Complaint Counsel subpoenaed deposition testimony and documents from Tiversa through Tiversa's chief executive officer and deposition designee, Mr. Robert Boback, and then relied on this evidence to claim that the 1718 File, which formed the basis for one of the two "security incidents" alleged in the Complaint, "has been found on a public P2P network as recently as November 2013. It has been downloaded from four different Internet Protocol ('IP') addresses, including IP addresses with 'unrelated sensitive consumer information that could be used to commit identity theft.'"[6] Complaint Counsel's Pre-Trial Brief at 49 (citing CX0703 (Boback Dep.)). Complaint Counsel gave this Tiversa-provided information to its proffered consumer injury expert witness, Mr. Rick Kam, who relied on that information to support his opinion that consumers identified in the 1718 File are at "a significantly higher risk of identity crimes than the general public." CX0742 (Kam Expert Report at 18-19). Complaint Counsel's other proffered consumer injury expert, Mr. James Van Dyke, also relied on Mr.

[6] Although Complaint Counsel marked this statement in its Pre-Trial Brief as subject to *in camera* treatment, the substance of this statement does not meet the Commission's strict standards for *in camera* treatment. The ALJ may disclose *in camera* material to the extent necessary for the proper disposition of the proceeding. 16 C.F.R. § 3.45(a); *In re General Foods Corp*., 95 F.T.C. 352, 356 n.7, 1980 FTC LEXIS 99, at *11 n.7 (March 10, 1980) (ALJs "retain the power to reassess prior *in camera* rulings at the time of publication of decisions."). In instances where a document or trial testimony had been given *in camera* treatment, but the portion of the material cited to in this Initial Decision does not in fact require *in camera* treatment, such material is disclosed in this public Initial Decision.

Boback's 2013 deposition testimony to support his projections of likely identity theft harm arising from the exposure of the 1718 File. CX0741 (Van Dyke Expert Report at 7-8, 12-14).

The credibility and reliability of evidence provided by Tiversa regarding the "spread" of the 1718 File, including to IP addresses allegedly belonging to identity thieves, began to unravel on May 30, 2014, shortly after Complaint Counsel had rested its case. Complaint Counsel announced in court that it had identified "a discrepancy" and a "misstatement on the record" of Mr. Boback's deposition "on which certain of our experts relied in making [consumer harm] calculations." Tr. 1227, *in camera*. Complaint Counsel requested to redepose Mr. Boback to allow him to revise his prior deposition testimony, and also requested leave to allow Complaint Counsel's consumer injury experts to revise their expert opinions based on Mr. Boback's anticipated revised testimony. These requests, made in the middle of trial, long after discovery had closed, and, indeed, after Complaint Counsel had rested its case, were denied. Tr. 1227-1229, *in camera*.[7]

Also on May 30, 2014, counsel for Respondent reported that the House Committee on Oversight and Government Reform ("OGR") had begun an investigation of Tiversa in conjunction with Tiversa's work with federal government agencies, and that Respondent's proposed witness for May 30, 2014, Tiversa's former employee, Mr. Richard Wallace, had just been informed by OGR that OGR was seeking to interview Mr. Wallace. Tr. 1225, *in camera*; *see* JX0003. It was further disclosed that, if called to testify in the administrative proceedings, Mr. Wallace would invoke his constitutional privilege against self-incrimination, pending his

[7] Complaint Counsel further explained in court: "it is also the representation of Mr. Boback's counsel that he has looked for the [1718 F]ile more recently and found it more recently, and on that basis we would seek to take a second deposition of Mr. Boback." Tr. 1227-1228, *in camera*. Complaint Counsel's explanation in court clearly indicated that Mr. Boback's "misstatement" was in regard to *when* Tiversa allegedly searched peer-to-peer networks and found the 1718 File in "multiple locations" and not *whether* Tiversa had in fact located the file in "multiple locations." Moreover, notwithstanding the denial of Complaint Counsel's request to redepose Mr. Boback, Complaint Counsel, over Respondent's objection, elicited testimony from Mr. Boback at Respondent's June 7, 2014 trial deposition of Mr. Boback (a deposition which was allowed due to Mr. Boback's alleged unavailability to appear at trial (Tr. 1251-1252)), that Tiversa ran a search for the 1718 File on June 3 or 4, 2014, and identified three IP addresses from which the 1718 File had been downloaded, in addition to the four IP addresses on CX0019 (discussed *infra* II.D.3.). RX0541 (Boback Trial Dep.) at 78. Because, as shown *infra*, Mr. Boback's testimony in this case is not credible, and evidence produced by Tiversa is not reliable as to the "spread" of the 1718 File, ultimately such "clarifying" testimony or evidence from Mr. Boback on this issue would not have been entitled to, or given, any weight.

effort to obtain a grant of prosecutorial immunity. Tr. 1225, 1231-1232, 1241-1242, *in camera*; *see* 16 C.F.R. § 3.39.

On June 12, 2014, counsel for Respondent stated on the record that Mr. Wallace was expected to testify in this case that the Tiversa-provided evidence that the 1718 File had been found at four IP addresses other than LabMD's, including IP addresses of identity thieves, had been manufactured, and that, in fact, the 1718 File had not been found at any IP address other than LabMD's. Tr. 1293. Also on June 12, 2014, Mr. Wallace took the stand and invoked his privilege against self-incrimination in response to Respondent's questioning. Tr. 1301-1302.

Proceedings were recessed to allow Mr. Wallace to seek prosecutorial immunity for the OGR testimony and for testimony in these administrative proceedings. *In re LabMD, Inc.*, 2014 FTC LEXIS 246 (Oct. 9, 2014). On December 29, 2014, on Respondent's motion, and pursuant to authority granted by the Attorney General of the United States on November 14, 2014, an Order was issued granting Mr. Wallace immunity pursuant to Commission Rule 3.39 and directing Mr. Wallace to testify in these proceedings. *See In re LabMD, Inc.*, 2014 FTC LEXIS 314 (Dec. 29, 2014). Proceedings reconvened for Mr. Wallace's testimony on May 5, 2015.[8]

On May 5, 2015, Mr. Wallace appeared and testified. As detailed in Section II.D.3., *infra*, Mr. Wallace testified that Tiversa's business model was to "monetize" documents that it downloaded from peer-to-peer networks, by using those documents to sell data security remediation services to the affected business, including by representing to the affected business that the business' information had "spread" across the Internet via peer-to-peer sharing networks, when such was not necessarily the case, and by manipulating Tiversa's internal database of peer-to-peer network downloads (the "Data Store") to make it appear that a business' information had been found at IP addresses belonging to known identity thieves. Mr. Wallace further testified that these practices were followed with regard to Tiversa's discovery of LabMD's 1718 File. In order to retaliate against LabMD for refusing to purchase Tiversa's services, Mr. Wallace

[8] Although proceedings were to reconvene on March 3, 2015, Mr. Wallace was granted two continuances. *See* Orders of February 24, 2015 and March 4, 2015. On March 12, 2015, the Administrative Law Judge ordered a further continuance *sua sponte* until May 5, 2015.

testified, Tiversa reported its discovery of the 1718 File to the FTC; and Mr. Wallace, at the direction of Mr. Boback, manipulated Tiversa's Data Store to make it appear that the 1718 File had been found at four IP addresses, including IP addresses of known identity thieves, and fabricated a list of those IP addresses, which Complaint Counsel introduced into evidence as CX0019.

Complaint Counsel opted not to take Mr. Wallace's deposition after his direct testimony. Tr. 1459. That deposition had been allowed by Order issued December 8, 2014. *In re LabMD, Inc.*, 2014 FTC LEXIS 307 (Dec. 8, 2014). Complaint Counsel also chose not to cross-examine Mr. Wallace. Tr. 1459. Complaint Counsel further decided not to offer any rebuttal to Mr. Wallace's testimony. Tr. 1459. *See* Complaint Counsel's Notice Regarding Rebuttal, May 12, 2015.[9]

Meanwhile, the OGR's investigation of Tiversa continued, including with respect to Tiversa's dealings with the FTC in this case. *See* RX0542; RX0543. An OGR staff report, dated January 2, 2015, but not released until after the completion of Mr. Wallace's testimony in this matter, concluded, *inter alia*, that Tiversa and Mr. Boback provided incomplete, inconsistent, and/or conflicting information to the FTC for this case. *See* RX0644; *see also In re LabMD, Inc.*, 2015 FTC LEXIS 175 (July 15, 2015).

On June 24, 2015, Complaint Counsel announced for the first time that it "does not intend to cite to Mr. Boback's testimony or CX0019 in its proposed findings of fact. Nor does Complaint Counsel intend to cite to expert conclusions predicated on Mr. Boback's testimony or CX0019." Complaint Counsel's Opposition to Respondent's Motion to Admit Exhibits at 10-11 n.11. *See also* Complaint Counsel's Response to Respondent's Motion to Refer Tiversa and Boback for Criminal Investigation at 2 n.1 (July 1, 2015).[10] Complaint Counsel further explained its retreat from Tiversa-provided evidence in its Post-Trial Brief, stating: "The

[9] Complaint Counsel's Motion to Issue Subpoenas to Tiversa to develop rebuttal evidence, filed July 8, 2014, before Mr. Wallace's testimony and while Mr. Wallace's request for immunity was still pending with the Attorney General, had been denied as premature. *In re LabMD, Inc.*, 2014 FTC LEXIS 194 (July 23, 2014).

[10] Complaint Counsel did not oppose a criminal referral of Tiversa and Mr. Boback; however, Respondent's motion for such referral was denied for failure to provide sufficient legal authority. *In re LabMD, Inc.*, 2015 FTC LEXIS 177 (July 15, 2015).

assertions made on page 49 of Complaint Counsel's pre-trial brief are not repeated here. Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony." Complaint Counsel's Post-Trial Brief at 61 n.3.[11] However, as shown *infra*, Complaint Counsel does rely on expert opinions that were predicated on Mr. Boback's testimony. In addition, Complaint Counsel relies on Mr. Boback's deposition testimony to counter Respondent's Proposed Findings of Fact. *See, e.g.*, CCRRFF 72b, 73b, 74b.

C. EVIDENCE

This Initial Decision is based on a consideration of the whole record relevant to the issues, including the exhibits properly admitted into evidence, deposition transcripts, and the transcripts of testimony at trial, and addresses the material issues of fact and law. The briefs and proposed findings of fact and conclusions of law, and the replies thereto, submitted by the parties, and all contentions and arguments therein were thoroughly reviewed and considered.

Proposed findings of fact submitted by the parties but not accepted in this Initial Decision were rejected, either because they were not supported by the evidence or because they were not dispositive or material to the determination of the merits of the case. Similarly, legal contentions and arguments of the parties that are not addressed in this Initial Decision were rejected, because they lacked support in fact or law, were not material, or were otherwise lacking in merit.[12]

[11] The parties filed corrected versions of some of their post-trial filings, as indicated in footnote 13. Citations in this Initial Decision to those filings are to the corrected version of the filing.

[12] Ruling upon a decision of the Interstate Commerce Commission, and interpreting language in the Administrative Procedure Act that is almost identical to language in FTC Rule 3.51(c)(1), the United States Supreme Court held that "[b]y the express terms of [that Act], the Commission is not required to make subordinate findings on every collateral contention advanced, but only upon those issues of fact, law, or discretion which are 'material.'" *Minneapolis & St. Louis Ry. Co. v. United States*, 361 U.S. 173, 193-94 (1959). *Accord Stauffer Labs., Inc. v. FTC*, 343 F.2d 75, 82 (9th Cir. 1965). *See also Borek Motor Sales, Inc. v. NLRB*, 425 F.2d 677, 681 (7th Cir. 1970) (holding that it is adequate for the Board to indicate that it had considered each of the company's exceptions, even if only some of the exceptions were discussed, and stating that "[m]ore than that is not demanded by the [APA] and would place a severe burden upon the agency"). Furthermore, the Commission has held that Administrative Law Judges are not required to discuss the testimony of each witness or all exhibits that are presented during the administrative adjudication. *In re Amrep Corp.*, 102 F.T.C. 1362, 1670, 1983 FTC LEXIS 17, at *566-67 (Nov. 2, 1983).

Under Commission Rule 3.51(c)(1), "[a]n initial decision shall be based on a consideration of the whole record relevant to the issues decided, and shall be supported by reliable and probative evidence." 16 C.F.R. § 3.51(c)(1); *see In re Chicago Bridge & Iron Co.*, 138 F.T.C. 1024, 1027 n.4, 2005 FTC LEXIS 215, at *3 n.4 (Jan. 6, 2005). Under the Administrative Procedure Act ("APA"), an Administrative Law Judge may not issue an order "except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence." 5 U.S.C. § 556(d). All findings of fact in this Initial Decision are supported by reliable, probative, and substantial evidence. Citations to specific numbered findings of fact in this Initial Decision are designated by "F."[13]

Pursuant to Commission Rule 3.45(b), several orders were issued in this case granting *in camera* treatment to material, after finding, in accordance with the Rule, that its public disclosure would likely result in a clearly defined, serious injury to the entity requesting *in camera* treatment or that the material constituted "sensitive personal information," as that term is defined in Commission Rule 3.45(b). This Initial Decision does not disclose any *in camera* information and there is only a public version of the Initial Decision.

[13] References to the record are abbreviated as follows:

CCX – Complaint Counsel's Exhibit
RX – Respondent's Exhibit
JX – Joint Exhibit
Tr. – Transcript of testimony before the Administrative Law Judge
Dep. – Transcript of Deposition
CCB – Complaint Counsel's Corrected Post-Trial Brief
CCRB – Complaint Counsel's Post-Trial Reply Brief
CCFF – Complaint Counsel's Proposed Findings of Fact
CCRRFF – Complaint Counsel's Reply to Respondent's Proposed Findings of Fact
CCCL – Complaint Counsel's Conclusions of Law
RB – Respondent's Corrected Post-Trial Brief
RRB – Respondent's Post-Trial Reply Brief
RFF – Respondent's Proposed Findings of Fact
RRCCFF – Respondent's Reply to Complaint Counsel's Proposed Findings of Fact
RCL – Respondent's Corrected Conclusions of Law

D. SUMMARY OF INITIAL DECISION

Section 5(n) of the FTC Act states that "[t]he Commission shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless [1] the act or practice causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Complaint Counsel has failed to carry its burden of proving its theory that Respondent's alleged failure to employ reasonable data security constitutes an unfair trade practice because Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.

First, with respect to the 1718 File, the evidence fails to prove that the limited exposure of the 1718 File has resulted, or is likely to result, in any identity theft-related harm, as argued by Complaint Counsel. Moreover, the evidence fails to prove Complaint Counsel's contention that embarrassment or similar emotional harm is likely to be suffered from the exposure of the 1718 File alone. Even if there were proof of such harm, this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a "substantial injury" within the meaning of Section 5(n).

Second, with respect to the exposure of certain LabMD "day sheets" and check copies, Complaint Counsel has failed to prove that the exposure of these documents is causally connected to any failure of Respondent to reasonably protect data maintained on its computer network, as alleged in the Complaint, because the evidence fails to show that these documents were maintained on, or taken from, Respondent's computer network. In addition, Complaint Counsel has failed to prove that this exposure has caused, or is likely to cause, any consumer harm.

Third, Complaint Counsel's argument that identity theft-related harm is likely for all consumers whose personal information is maintained on LabMD's computer networks, even if their information has been not exposed in a data breach, on the theory that LabMD's computer networks are "at risk" of a future data breach, is rejected. In summary, the evidence fails to

assess the degree of the alleged risk, or otherwise demonstrate the probability that a data breach will occur. To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical "risk" of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of "likely" substantial consumer injury.

At best, Complaint Counsel has proven the "possibility" of harm, but not any "probability" or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case. Accordingly, the Complaint is DISMISSED. Because Complaint Counsel has failed to prove its case on the merits, it is not necessary to address Respondent's affirmative defenses set forth in the Amended Answer.

II. FINDINGS OF FACT

A. KEY TERMS

1. **1718 File**: The LabMD Insurance Aging report, containing 1,718 pages, with the filename "insuranceaging_6.05.071.pdf" that is identified as the "P2P [peer-to-peer] insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint, a copy of which is designated as CX0697 (*in camera*), and a redacted copy of which is designated at RX0072. (Joint Stipulations of Fact, JX0001-A at 1).

2. **Consumer**: A natural person. The patients of LabMD's physician clients are consumers, as that term is used in Section 5(n) of the Federal Trade Commission Act, 15 U.S.C. § 45(n). (Joint Stipulations of Fact, JX0001-A at 1, 2).

3. **Personal Information ("PI")**: Individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number ("SSN"); (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. (Joint Stipulations of Fact, JX0001-A at 1-2).

B. TESTIFYING EXPERTS

1. Complaint Counsel's Experts

a. Dr. Raquel Hill

4. Dr. Raquel Hill is a tenured professor of computer science at Indiana University with over 25 years of experience in computing, with expertise in computer security, data privacy, and networking systems. (CX0740 (Hill Expert Report ¶ 1)).

5. Dr. Hill has a Ph.D. in computer science from Harvard University. She has designed and taught classes in information and systems security. (CX0740 (Hill Expert Report ¶¶ 8, 9)).

6. Dr. Hill was asked to assess whether LabMD provided reasonable security for Personal Information within its computer network, and whether any alleged security failures could have been corrected using readily available security measures. Specifically, Dr. Hill was asked to analyze the record evidence relating to the allegations in paragraphs 10 and 11 of the Complaint. (CX0740 (Hill Expert Report ¶¶ 2, 45)).

7. Dr. Hill's conclusions in this case are limited to the time period from January 2005 through July 2010 (the "Relevant Time Period"). Dr. Hill found insufficiently "diverse types of information available" after the Relevant Time Period to offer any opinions after the Relevant Time Period, and did not offer any opinions on the reasonableness of LabMD's security practices after July 2010. (CX0740 (Hill Expert Report ¶¶ 4, 48); Hill, Tr. 84-85, 203).

8. Dr. Hill was asked to evaluate and opine on the expert report of Respondent's expert, Mr. Adam Fisk (F. 20). Specifically, Dr. Hill was asked to opine on Mr. Fisk's rebuttal to Dr. Hill's expert report and Mr. Fisk's opinions regarding LabMD's network security practices. (CX0737 (Hill Rebuttal Expert Report) ¶ 2).

b. Mr. Rick Kam

9. Mr. Rick Kam is a Certified Information Privacy Professional. He is president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. (CX0742 (Kam Expert Report at 3)).

10. Mr. Kam leads and participates in cross-industry data privacy groups, publishes relevant articles in the field, and works on development of policy and solutions to address the protection of health information and personally identifiable information. Mr. Kam's expertise includes "identifying and remediating the consequences of identity theft and medical identity theft" and "helping organizations develop policies and solutions" to safeguard sensitive personal information. (CX0742 (Kam Expert Report at 3-5, 25, 29-33)).

11. Mr. Kam was asked to "assess the risk of injury to consumers caused by the unauthorized disclosure of [consumers'] sensitive personal information." (CX0742 (Kam Expert Report at 5)).

c. Mr. James Van Dyke

12. Mr. James Van Dyke is the founder and president of Javelin Strategy & Research ("Javelin"), which performs independent research on customer-related security, fraud, payments, and electronic financial services. Mr. Van Dyke has extensive experience in conducting surveys. He leads the publication of an annual, nationally representative victim study of identity crimes in the United States. (Van Dyke, Tr. 574-576, 580-581; CX0741 (Van Dyke Expert Report at 1)).

13. Mr. Van Dyke makes presentations on secure personal financial management, identity fraud, and payments and security to groups including the U.S. House of Representatives, Federal Reserve Bank gatherings, and the RSA Security Conference. (CX0741 (Van Dyke Expert Report at 1)).

14. Mr. Van Dyke's expertise includes consumer behavior, security technologies, personal financial services and payments, how sensitive information is used, and identity theft. (CX0741 (Van Dyke Expert Report at 1-2)).

15. Mr. Van Dyke was asked to "assess the risk of injury to consumers whose personally identifiable information (PII)[[14]] has been disclosed by [LabMD] without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure." (CX0741 (Van Dyke Expert Report at 2)).

d. Dr. Clay Shields

16. Dr. Clay Shields is a tenured professor in the computer science department of Georgetown University, with expertise in networking and network protocols, computer security, digital forensics, and responding to network and computer system events. (CX0738 (Shields Rebuttal Expert Report ¶ 1)).

17. Dr. Shields has over 20 years of computer science experience, including in digital forensics research and developing and analyzing network protocols. (CX0738 (Shields Rebuttal Expert Report ¶ 5)).

18. Dr. Shields' research includes work on systems for providing anonymity to users through peer-to-peer technology. He was involved in a collaborative effort that resulted in a modified Gnutella client that is widely used by law enforcement.[15] (CX0738 (Shields Rebuttal Expert Report ¶¶ 7, 9)).

19. Dr. Shields was asked to review the expert report of Respondent's expert, Mr. Adam Fisk (F. 20), and provide opinions about Mr. Fisk's conclusions concerning the LimeWire peer-to-peer file-sharing program[16] and the alleged disclosure of the 1718 File. (CX0738 (Shields Rebuttal Expert Report ¶ 2)).

2. Respondent's Expert

a. Mr. Adam Fisk

20. Mr. Adam Fisk is the president and chief executive officer of the Brave New Software Project, Inc., the creators of Lantern, a peer-to-peer tool for bypassing government censors in countries such as Iran and China that censor citizens' access to the Internet. Mr. Fisk is the former lead engineer at LimeWire LLC, the creators of the LimeWire file-

[14] Personally Identifiable Information ("PII") is a subset of the data in Personal Information (F.3) and includes a person's name, address, date of birth, Social Security number, credit card and banking information, and drivers' license number. (CX0742 (Kam Expert Report at 10)).

[15] Peer-to-peer technology and the Gnutella client are discussed *infra* II.D.1.

[16] The LimeWire peer-to-peer file-sharing program is discussed *infra* II.D.1.

sharing application, and has extensive experience in peer-to-peer software, computer networking, and data security, including 13 years of professional experience building peer-to-peer applications, with a focus on computer networking and security. (RX0533 (Fisk Expert Report at 3-4)).

21. Mr. Fisk was asked to provide an opinion as to whether LabMD provided adequate security to secure Protected Health Information[17] contained within its computer network from January 2005 through July 2010 (the "Relevant Time Period" assessed by Dr. Hill). Mr. Fisk also provided his review of LimeWire functionality, an analysis of LabMD's network, an analysis of the 1718 File on the LabMD network, and a rebuttal to the expert report of Dr. Hill. (RX0533 (Fisk Expert Report at 3-4)).

22. Mr. Fisk based his opinions of the facts of this case on his extensive experience and documents provided to him by Respondent. (RX0533 (Fisk Expert Report at 3-4, 37)).

23. In forming his opinions, Mr. Fisk considered an analysis of the equipment LabMD had in place, including whether or not LabMD had firewalls in place, an analysis of the depositions describing the network and the practices in place at the company, and an analysis of a report conducted for LabMD by an outside contractor that looked at any vulnerabilities on LabMD's network. (Fisk, Tr. 1158-1159).

C. RESPONDENT

1. Background Information

24. LabMD is a privately held Georgia corporation, incorporated in 1996 by Mr. Michael J. Daugherty. (Daugherty, Tr. 939; CX0766 at 2).

25. Mr. Daugherty is the sole owner of LabMD and is its president and chief executive officer. (Daugherty, Tr. 936; CX0709 (Daugherty, Dep. at 12)).

26. From at least 2001 through approximately December 2013 or January 2014, LabMD was in the business of conducting clinical laboratory tests on urological specimen samples from patients and reporting test results to physician customers. (Answer ¶ 3; CX0766 at 3; CX0291; Daugherty, Tr. 952).

27. During the period LabMD was operational (F. 26, 39), LabMD operated as a small, medical services company providing uro-pathology cancer detection services to urologists who wanted their patients' tissue samples analyzed by pathologists who specialized in prostate cancer or bladder cancer. (Daugherty, Tr. 941-943, 952).

[17] Protected Health Information, as defined in 45 C.F.R. § 160.103, is a subset of the data in Personal Information. (Joint Stipulations of Fact, JX0001-A at 1, 2).

28. During the period LabMD was operational (F. 26, 39), LabMD tested samples from patients in multiple states, including Alabama, Mississippi, Florida, Georgia, Missouri, Louisiana, and Arizona. (Answer ¶ 5; CX0766 at 3).

29. The patients whose samples LabMD tested and from whom LabMD collected payments were located throughout the United States. (CX0766 at 3; CX0088, *in camera* (LabMD Copied Checks); CX0726 (Maxey, SUN Designee, Dep. at 17); CX0718 (Hudson, Dep. at 15-17); CX0722 (Knox, Dep. at 19); CX0706 (Brown, Dep. at 16-18); CX0715-A (Gilbreth, Dep. at 50-51); CX0713-A (Gardner, Dep. at 25-26)).

30. The acts and practices of Respondent alleged in the Complaint were in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44. (Joint Stipulations of Fact, JX0001-A at 1).

31. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35-40 million. (Daugherty, Tr. 1059; CX0709 (Daugherty, Dep. at 127-128)).

32. LabMD's peak annual revenue was approximately $10 million. (CX0709 (Daugherty, Dep. at 128)).

33. From 2005 through 2012, LabMD's approximate blended profit margin was 25%. (Daugherty, Tr. 1058-1059).

34. In 2013, LabMD's revenue was approximately $2 million. (CX0709 (Daugherty, Dep. at 128)).

35. LabMD's principal place of business from April 2009 through approximately January 2014 was 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339. (Answer ¶ 1; CX0766 at 2).

36. In January 2014, LabMD began winding down its operations. At that time, LabMD stopped accepting specimen samples and conducting tests. (CX0765 at 6; CX0710-A (Daugherty, LabMD Designee, Dep. at 195); CX0725-A (Martin, Dep. at 25)).

37. LabMD notified its physician clients by letter dated January 6, 2014, that it would not be accepting new specimens after January 11, 2014, and that all test results would be provided in the following week. LabMD further told its physician clients that LabMD would be closed for telephone calls and internet access after January 15, 2014, and that for the remainder of 2014, requests for past results or to obtain specimens for second opinions, could be made by facsimile. In addition, the January 6, 2014 letter stated, "billing operations" would continue through 2014. (CX0291; Daugherty, Tr. 1031).

38. After January 2014, in order to obtain an historical result report, as referred to in F. 37, the physician client had to send a facsimile requesting the results and LabMD would then fax the report back to the physician client. (CX0725-A (Martin, Dep. at 20)).

39. As of the start of the evidentiary hearing, May 2014, LabMD's operations were limited to preserving tissue samples for LabMD's physician clients, so the physicians could send out slides for second opinions, and to providing test results to physicians if they did not have them. (Daugherty, Tr. 1031; CX0291).

40. LabMD has continued to possess its computer equipment; its "Lytec" server (on which LabMD's electronic billing records are stored); and the laboratory information system (on which LabMD's electronic medical records are stored). Both of these servers can be turned on. (CX0709 (Daugherty, Dep. at 22-23); CX0766 at 2-3). *See also* CX0725-A (Martin, Dep. at 11-12); CX0705-A (Bradley, Dep. at 20)).

41. As of May 2014, LabMD continues to exist as a corporation, with Mr. Daugherty as it sole employee. (Daugherty, Tr. 1031; CX0291).

2. Collection of Personal Information in Connection with Lab Testing

42. In connection with performing tests, LabMD has collected and continues to maintain Personal Information for over 750,000 consumers. (Joint Stipulations of Fact, JX0001-A at 3; CX0765 at 10-11; CX0766 at 5; CX0710-A (Daugherty, LabMD Designee, Dep. at 193-194); CX0709 (Daugherty, Dep. at 21-23)).

43. In connection with performing tests for its physician clients, LabMD's Information Technology ("IT") staff set up data transfer of patients' Personal Information from LabMD's physician clients' databases to LabMD. (CX0718 (Hudson, Dep. at 36-39)).

44. The Personal Information that physicians transferred to LabMD included names, addresses, dates of birth, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. (CX0717 (Howard, Dep. at 34-35, 38); CX0718 (Hudson, Dep. at 59-60, 62); CX0726 (Maxey, SUN Designee, Dep. at 41-42); CX0728 (Randolph, Dep. at 48, 50-51)).

45. Patient Personal Information typically was transmitted to LabMD using a secure file transfer protocol, through which information flowed from the doctors' offices to a LabMD server on its network. (CX0711 (Dooley Dep. at 131-132); CX0730 (Simmons, Dep. at 61, 128); CX0717 (Howard, Dep. at 34-37, 54); CX0724 (Maire, Dep. at 41-43); CX0725-A (Martin, Dep. at 56-60)).

46. Once consumers' Personal Information was loaded in LabMD's laboratory application, LabSoft, staff at the physician clients' practice could order tests for the patients through LabSoft using LabMD's online portal by searching for the patient's name, selecting the correct patient from a list of patients in that practice, and entering the current procedural terminology ("CPT") code for the testing ordered. (CX0718 (Hudson, Dep. at 24-25); CX0709 (Daugherty, Dep. at 86-87); CX0725-A (Martin, Dep. at 56-57)).

47. A doctor's office employee could search by name, date of birth, or Social Security number to find a patient's record to order a test. (CX0726 (Maxey, SUN Designee, Dep. at 40, 47-48)).

48. When a doctor's office made a request for a test, a report and labels for the specimen would be printed at the doctor's office. The patient's specimen and the report were then sent to LabMD via Federal Express. (CX0725-A (Martin, Dep. at 56-57)).

49. Once a LabMD pathologist read a specimen and had a test result, the result was entered into a database. (CX0711 (Dooley Dep. at 132-133); CX0717 (Howard, Dep. at 49-50)).

50. The results from the tests LabMD performed could be accessed by LabMD's physician clients through a web portal using a user ID and password through LabMD-provided computers or the doctors' offices own computers. (CX0726 (Maxey, SUN Designee, Dep. at 29-31, 48-49); CX0728 (Randolph, Dep. at 21-22, 57-58); CX0704-A (Boyle, Dep. at 16, 22-23); CX0722 (Knox, Dep. at 76-78); CX0717 (Howard, Dep. at 59-60); Daugherty, Tr. 977).

51. In some instances, LabMD supplied computer equipment to doctors' offices, including computers, monitors, bar coder machines, and printers. (CX0730 (Simmons, Dep. at 61-62); CX0726 (Maxey, SUN Designee, Dep. at 23-24, 21, 27-28); CX0728 (Randolph, Dep. at 27-31, 42); CX0717 (Howard, Dep. at 59); CX0709 (Daugherty, Dep. at 83)).

3. Insurance Aging Reports

52. Insurance aging reports are spreadsheets of insurance claims and payments, which may include consumers' names, dates of birth, and Social Security numbers; the CPT codes for the laboratory tests conducted; and health insurance company names, addresses, and policy numbers. (Answer ¶ 9(a); CX0706 (Brown, Dep. at 54)).

53. Insurance aging reports were generated by LabMD's billing department to show accounts receivable that had not been paid and so that billing staff could attempt to collect payments on outstanding claims from patients' insurance companies. (CX0706 (Brown, Dep. at 20); CX0714-A ([Former LabMD Employee],[18] Dep. at 48-49)).

54. Insurance aging reports were based on a report from LabMD's Lytec billing system that displayed past-due payments from insurance companies. (CX0706 (Brown, Dep. at 23-24); CX0714-A ([Former LabMD Employee], Dep. at 52)).

55. Insurance aging reports were saved to the billing manager's workstation. (Daugherty, Tr. 982).

[18] By Order dated May 6, 2014, and for the reasons stated therein, *in camera* treatment was granted to the name of one particular former LabMD employee in the billing department. Disclosure of this employee's name is not necessary for the proper disposition of the proceeding and therefore it is replaced with the designation "[the Former LabMD Employee]" in this Initial Decision.

56. [The Former LabMD Employee] (*see* footnote 18) received hard copies of insurance aging reports from LabMD's billing manager every month. Based on the information in the report, the employee would contact the insurance company, obtain the status of the denied claim, and attempt to find ways for the insurance company to pay the claim. (CX0714-A ([Former LabMD Employee], Dep. at 49-50)).

4. Collection of Personal Information in Connection with Payments

57. Insured patients could pay the part of LabMD's charges not covered by insurance, and uninsured patients could be responsible for the full amount of the charges. (Answer ¶ 4).

58. Consumers could pay LabMD's charges with credit cards, debit cards, or personal checks. (CX0766 at 6; CX0706 (Brown, Dep. at 39-40); CX0765 at 8).

59. When consumers paid LabMD by credit card, the billing department ran the credit card number and posted the payment in LabMD's system. (CX0716 (Harris, Dep. at 20-21)).

60. When consumers paid LabMD by check or money order and LabMD received that payment by mail, it was LabMD's practice for LabMD staff to make a photocopy of the check or money order. LabMD did not scan checks or money orders in the 2005 to 2010 time period. (CX0716 (Harris, Dep. at 23-24, 27); CX0706 (Brown, Dep. at 28-29); CX0715-A (Gilbreth, Dep. at 50-51)).

61. When consumers paid LabMD by check or money order, the photocopy (F. 60) would be given to the billing department. The billing department would post the payment and retain the photocopy of the check. Original checks were kept for six months, and then were shredded. (CX0713-A (Gardner, Dep. at 26-27)).

62. Personal checks contain a consumer's account number, bank routing number, signature, and often an address and phone number. (*E.g.*, CX0088, *in camera* (LabMD Copied Checks)).

D. THE 1718 FILE INCIDENT

1. Peer-to-Peer Networks

63. Peer-to-peer file-sharing applications enable one computer user to make a request to search for all files that have been made available for sharing by another (or "host") computer that is also using the file-sharing application. (Hill, Tr. 119-120; Shields, Tr. 826; CX0738 (Shields Rebuttal Expert Report ¶¶ 15, 18)).

64. Peer-to-peer networks are often used to share music, videos, pictures, and other materials. (CX0738 (Shields Rebuttal Expert Report ¶ 14); Answer ¶ 13; CX0740 (Hill Expert Report ¶ 42); Shields, Tr. 851).

65. Typically, users will perform a search using terms related to the particular file they hope to find and receive a list of possible matches. The user then chooses a file they want to download from the list. This file is then downloaded from other peers who possess that file. (CX0738 (Shields Rebuttal Expert Report ¶ 18)).

66. A document being "shared" or "made available for sharing" on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. The fact that a document is being shared, or made available for sharing, does not mean the document has been "downloaded" for viewing. (Shields, Tr. 891-892).

67. It is very difficult for a user to know what is in a document found on a peer-to-peer network without downloading and opening the document. (Wallace Tr. 1343).

68. The contents of a file that is available for sharing are not disclosed until the file is downloaded and viewed. (F. 65-67).

69. LimeWire is a peer-to-peer file-sharing application that can be used to transport files across the Internet. LimeWire is one of a number of applications that use a protocol called Gnutella (F. 70). (RX0533 (Fisk Expert Report at 9)).

70. Gnutella is a program that connects computers together in a direct peer-to-peer fashion to facilitate file sharing through searching and downloading. (RX0533 (Fisk Expert Report at 9); CX0738 (Shields Rebuttal Expert Report ¶17)).

71. A Gnutella "client" refers to the piece of software that understands the Gnutella protocol and allows a peer to interact with other peers using the Gnutella protocol. (Shields, Tr. 827).

72. In order to share a file or folder on LimeWire, the user must actively choose the file or folder to share. (RX0533 (Fisk Expert Report at 10)).

73. The 1718 File, discussed *infra* Section II.D.2., has the computer filename "insuranceaging_6.05.071.pdf". (F. 1, 78).

74. When a user makes a file available for sharing on LimeWire, LimeWire breaks apart the file names into keywords to allow other users to search for them. (RX0533 (Fisk Expert Report at 11, 13)).

75. In this case, LimeWire would break apart the "insuranceaging_6.05.071.pdf" file name into the keywords "insuranceaging" and "6.05.071" because LimeWire only recognizes the "_" as a word delimiter and does not recognize that "insuranceaging" is, in fact, the words "insurance" and "aging" merged together. (Fisk, Tr. 1154-1156; RX0533 (Fisk Expert Report at 11-12)).

76. A search for "insurance" or for "aging" would not return a search result for "insuranceaging_6.05.071.pdf". (Fisk, Tr. 1155-1156; RX0533 (Fisk Expert Report at 11-12)).

77. In order for a searcher to receive a search result for the "insuranceaging_6.05.071.pdf" file, he or she would have to enter the search terms "insuranceaging" or "6.05.071". Both of those searches are highly unusual, and it is extremely unlikely that any LimeWire user would ever enter them. (Fisk, Tr. 1155-1156; RX0533 (Fisk Expert Report at 11-12)).

2. The 1718 File

a. Background facts

78. The "1718 File" is a LabMD insurance aging report, containing 1,718 pages, dated June 2007, with the filename "insuranceaging_6.05.071.pdf". (F. 1; Joint Stipulations of Fact, JX0001-A at 1; CX0697, *in camera* (1718 File)). The peer-to-peer sharing and subsequent disclosure of the 1718 File is referred to herein as the "1718 File Incident."

79. The 1718 File was created and stored on a LabMD computer. (Daugherty, Tr. 1078-1079).

80. The 1718 File had been maintained on the LabMD computer used by LabMD's billing manager, Ms. Rosalind Woodson ("Billing Computer"). (CX0766 at 9; Daugherty, Tr. 1079).

81. The 1718 File is a billing file generated from LabMD's billing application, the Lytec system. (CX0709 (Daugherty, Dep. at 146); CX0736 (Daugherty, IHT at 83-84); CX0706 (Brown, Dep. at 23-24)).

82. The 1718 File contains the following Personal Information for approximately 9,300 consumers: names; dates of birth; nine digit numbers that appear to be Social Security numbers; CPT codes for laboratory tests conducted; and, in some instances, health insurance company names, addresses, and policy numbers. (CX0766 at 8; Answer ¶ 19; CX0697, *in camera*).

83. The CPT number is a code used for the purpose of having a standardized description of procedures or tests provided for a patient. The CPT numbers do not disclose the laboratory test performed. Determining what test was performed, as reflected by the code, requires additional research, such as going to the website for the American Medical Association or performing a Google search for the code, which is how Mr. Kam, Complaint Counsel's expert, determined the tests reflected by the CPT codes in the 1718 File. (Kam, Tr. 445-447).

84. At the time the 1718 File was downloaded by Tiversa Holding Company ("Tiversa") in February 2008 (*see* F. 121), the 1718 File was in the "My Documents" folder on LabMD's Billing Computer. (CX0710-A (Daugherty, LabMD Designee, Dep. at 200)).

85. In February 2008, the Billing Computer's "My Documents" folder was available for sharing on LimeWire. (CX0156; CX0730 (Simmons, Dep. at 12, 28-29, 32)).

86. Most of the 950 files in the "My Documents" folder on the Billing Computer that were available for sharing via LimeWire at or around the same time as the 1718 File were music or video files. (Answer ¶ 18(b); CX0154; CX0730 (Simmons, Dep. at 33-34)).

87. Eighteen documents were available for sharing in the "My Documents" folder on the Billing Computer at or around the same time as the 1718 File, three of which contained Personal Information. (Wallace, Tr. 1406-1407; RX0645 at 39, 42, 43, *in camera*).

b. LabMD discovery

88. In May 2008, Tiversa contacted LabMD and told LabMD that the 1718 File was available through LimeWire. (Answer ¶ 17; CX0766 at 8; Daugherty, Tr. 981; Joint Stipulations of Fact, JX0001-A at 4).

89. After being contacted by Tiversa in May 2008, LabMD investigated and determined that LimeWire had been downloaded and installed on the Billing Computer in 2005 or 2006. (Answer ¶ 18(a); CX0755 at 4; CX0150; CX0730 (Simmons, Dep. at 10); CX0709 (Daugherty, Dep. at 144); CX0766 at 8-9).

90. In May 2008, as part of LabMD's investigation, LabMD IT Specialist Alison Simmons inspected LabMD's computers manually to identify which computer(s) were sharing files on peer-to-peer network(s) and determined that LimeWire had been installed only on the Billing Computer. (CX0734 (Simmons, IHT at 14); CX0730 (Simmons, Dep. at 10)).

91. As part of LabMD's investigation regarding the 1718 File, Ms. Simmons took screenshots of the Billing Computer, which show the existence of LimeWire and the shared 1718 File. (CX0150; CX0151; CX0152; CX0154; CX0155; CX0156; CX0730 (Simmons, Dep. at 14-15, 21, 23-24, 27, 29, 36-37, 42, 112, 150-152)).

92. After taking the screenshots (F. 91), Ms. Simmons removed LimeWire from the Billing Computer in May 2008. (CX0730 (Simmons, Dep. at 14-15); Answer ¶ 20).

93. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons searched all computers at LabMD for file-sharing software. (CX0704 (Boyle, Dep. at 57-66, 74-88); CX0149; CX0150; CX0151; CX0152; CX0153; CX0154; CX0155; CX0156; CX0157).

94. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons did not find any file-sharing software on any LabMD computer other than the Billing Computer. (CX0730 (Simmons, Dep. at 10-11)).

95. Mr. John Boyle, LabMD's vice president of operations and general manager from November 1, 2006 until the end of August 2013, assigned Ms. Simmons, and later, IT Manager Jeffrey Martin, to search peer-to-peer networks to look for the 1718 File. (CX0704-A (Boyle, Dep. at 6-8; 63-64); CX0725-A (Martin, Dep. at 9)).

96. As part of LabMD's investigation regarding the 1718 File in May 2008, Ms. Simmons searched peer-to-peer networks from her home computer to look for the 1718 File. She searched multiple times for at least a month thereafter for the file name insuranceaging_6.05.071.pdf, partial file names, and anything with the name LabMD associated with it. (CX0730 (Simmons, Dep. at 17-18); CX0704-A (Boyle, Dep. at 63-64)).

97. As part of LabMD's investigation regarding the 1718 File, in 2013, Mr. Martin searched peer-to-peer networks for the 1718 File multiple times over the course of a few months, using the file name, and the terms "LabMD," "patient," and "aging." (CX0725-A (Martin, Dep. at 98-101); CX0704-A (Boyle, Dep. at 63-64)).

98. Through their searches (F. 96-97), Ms. Simmons and Mr. Martin were not able to find the 1718 File on any peer-to-peer networks. (CX0730 (Simmons, Dep. at 17-18); CX0725-A (Martin, Dep. at 100); CX0704-A (Boyle, Dep. at 63-64)).

99. The 1718 File was not available from LabMD's computers to be shared via any peer-to-peer networks after May 2008. (F. 92-98).

3. Tiversa

a. Tiversa's business

100. Tiversa Holding Company ("Tiversa") is a data security company that offers breach detection and remediation services. Essentially, Tiversa uses a series of algorithms to search the entire peer-to-peer network for documents of interest to its clients or potential clients, and downloads the documents that are found. (CX0703 (Boback, Tiversa Designee, Dep. at 10-12); RX0541 (Boback Trial Dep. at 19-21); Wallace Tr. 1339-1341).

101. Mr. Robert Boback is the chief executive officer of Tiversa. (CX0703 (Boback, Tiversa Designee, Dep. at 11)).

102. In July 2007, Mr. Boback hired Mr. Richard Wallace as a forensic analyst. (Wallace, Tr. 1337, 1339-1340).

103. As a forensic analyst for Tiversa, Mr. Wallace's job included writing up a narrative for clients or potential clients as to the type of information Tiversa found, where it was found, and who the disclosing source was. (Wallace, Tr. 1339-1341).

104. Mr. Wallace's job included searching peer-to-peer networks using a standard peer-to-peer Gnutella client, such as LimeWire or Kazaa, to supplement information that Tiversa's system may not have downloaded. As an example of a search, if Tiversa were looking for insurance information for a healthcare company, Mr. Wallace would conduct a search using words such as "insurance" or "report," or any word that would identify an exposed file. (Wallace Tr. 1342-1344).

105. Because it is very difficult to know what is in a document found on a peer-to-peer network without downloading and opening the document, Mr. Wallace would begin by viewing the file titles and Internet protocol ("IP") addresses[19] returned from a search. He would then download any and all information that was available from a search. (Wallace Tr. 1343-1345).

106. Tiversa maintained a depository of long servers to store data that Tiversa's searches "pulled down," or downloaded, from peer-to-peer networks, which is referred to as Tiversa's "data store" ("Data Store"). The Data Store contained copies of files that Tiversa had downloaded from the Gnutella network. The Data Store also contained information as to where the downloaded file had been located. (Wallace, Tr. 1345, 1371).

107. There are two ways for legitimate data to get into Tiversa's Data Store. Tiversa's program, Eagle Vision, will automatically download files returned from Tiversa's searches, or an analyst, such as Mr. Wallace, can insert data that the analyst has found using a stand-alone computer running a peer-to-peer client. (Wallace, Tr. 1389-1390).

108. Mr. Wallace's job as a forensic analyst included searching for exposed files on peer-to-peer networks, and recording the information disclosed, including the company that had the disclosure, and when the information was disclosed. This information would be included on a spreadsheet that Tiversa analysts would update several times a day. The purpose of the spreadsheet was so that Mr. Boback and the Tiversa sales force could make sales calls to the affected companies. (Wallace, Tr. 1437-1438).

109. When a document was downloaded by Tiversa, Tiversa would record information as to the IP address from which the document was downloaded. When contacting the affected company to sell services, Tiversa's practice was to not reveal the source of the information and to tell the potential client that the IP information had not been recorded by Tiversa. Tiversa would "strip" the IP address off the found documents and remove any metadata[20] relating to the disclosure source, while keeping a separate set of the files which included disclosure source information. (Wallace, Tr. 1344-1345, 1439-1440).

[19] Computers on the Internet are able to identify each other by the use of IP addresses. The IP address uniquely identifies each computer on a network. (Shields, Tr. 821-825).

[20] Metadata is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data. http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

110. When Mr. Wallace, or any other analyst at Tiversa, downloaded a file that was deemed significant, Mr. Boback would be advised, and Mr. Boback would make the decision as to how to proceed to "monetize" the file; *i.e.*, whether the information would be given to a salesperson, or whether Mr. Boback himself would contact the company, to try to sell Tiversa's services. (Wallace, Tr. 1344, 1360).

111. Tiversa would monetize information it obtained from peer-to-peer networks either by selling a monitoring contract, pursuant to which Tiversa would search for certain key words for a period of time, or by selling a "one-off" service, that would remediate just the existing disclosure problem. (Wallace, Tr. 1364).

112. A Tiversa monitoring services contract for a large financial company could cost as much as a million dollars per year, down to a few thousand dollars per month for monitoring contracts for small "mom and pop" companies. (Wallace, Tr. 1366).

113. Tiversa was having problems selling monitoring contracts, so Tiversa started contacting individual companies whose information Tiversa had discovered. Instead of a year-long monitoring contract, Tiversa could try to sell a less expensive one-time service to address the problem. This attempt to "monetize" the information through a "one-off" sale after Tiversa's discovery of information on a peer-to-peer network was known as an "incident response case," or "IRC." (Wallace, Tr. 1359-1361).

114. A hypothetical example of an IRC would be a company that had a single file exposed with 5,000 individuals' personal information, and that company would only need the name of the person exposing the file. (Wallace, Tr. 1360).

115. When a company refused to purchase Tiversa's services, Mr. Wallace observed that Mr. Boback would often respond, in reference to that company, to the effect of, "you think you have a problem now, you just wait." Thereafter, an analyst of Tiversa would input information into Tiversa's Data Store so as to make that company's information "proliferate" in Tiversa's Data Store and thereby make it appear that a file had "spread" to multiple places. Tiversa could use this Data Store "evidence" to follow up with a company to try again to get the company to purchase Tiversa's remediation services. (Wallace, Tr. 1364-1365).

116. If a potential Tiversa client would not purchase Tiversa's services, another way Tiversa would "monetize" peer-to-peer findings would be to notify an existing Tiversa client of the disclosing source of the client's information and advise the existing client to contact Tiversa's target. Tiversa could "strong-arm people that way as well." (Wallace, Tr. 1451-1452).

117. When a company refused to purchase Tiversa's services after being contacted by Tiversa about a disclosure, Tiversa would need an excuse to make contact with the company again, so it would contact the company to report that the file had proliferated, or

"spread," to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. (Wallace, Tr. 1366-1368).

118. Part of Mr. Wallace's job for Tiversa was to make it appear that a company's file had spread to more IP addresses, including to IP addresses of identity thieves. He did this by placing files he might have found outside Tiversa's searching system into a folder in the Data Store and making it appear that Tiversa had located and downloaded the file from the IP address of a known bad actor. As far as the Data Store sees it, the file was downloaded from that IP address, but in reality no data transferred. (Wallace, Tr. 1367-1368).

119. Tiversa's Data Store was a record of files that were found "live" on the Internet, but also included information designed to make it appear that files had been found at other locations on the Internet. (Wallace, Tr. 1441).

120. Tiversa's Data Store is not a credible or reliable source of information as to the disclosure source or the spread of any file purportedly found by Tiversa. (F. 106-109, 115, 117-119).

b. Tiversa's dealings with LabMD

121. On or about February 25, 2008, Mr. Wallace, on behalf of Tiversa, downloaded the 1718 File from a LabMD IP address in Atlanta, Georgia, designated as 64.190.82.42. (Wallace, Tr. 1395, 1410-1411, 1440-1441; CX0307).

122. The 1718 File was found by Mr. Wallace, and was downloaded from a peer-to-peer network, using a stand-alone computer running a standard peer-to-peer client, such as LimeWire. (Wallace, Tr. 1342-1343, 1371-1372, 1440-1441).

123. After locating the 1718 File on February 25, 2008, Mr. Wallace input the information in Tiversa's Data Store. (Wallace, Tr. 1441).

124. In 2008, CIGNA Health Insurance ("CIGNA") was a company for which Tiversa was providing peer-to-peer monitoring services. An "incident record form" was prepared by Tiversa for its then-client CIGNA, and was admitted into evidence as RX0545. (Wallace, Tr. 1449-1451; RX0545).

125. Tiversa's representation to its client CIGNA, in RX0545, that the 1718 File had been found on April 18, 2008 is not correct, but was part of Tiversa's practice of ensuring that information continually flows to clients, so that it would appear that Tiversa was getting things done for the client. (Wallace, Tr. 1449-1451; RX0545 at 1).

126. Within minutes of Mr. Wallace's opening the 1718 File, Mr. Boback was viewing the document over Mr. Wallace's shoulder. Mr. Wallace observed that Mr. Boback was excited about the find. (Wallace, Tr. 1442).

127. Using the "browse host" [21] function, Mr. Wallace also downloaded 18 other LabMD documents in addition to the 1718 File, three of which contained Personal Information. (Wallace, Tr. 1372, 1400-1401, 1404-1406, 1415; *see* RX0645, *in camera* (LabMD Documents produced by Wallace at 39, 42-43)).

128. In May 2008, Tiversa began contacting LabMD to try to sell Tiversa's remediation services to LabMD. These efforts included representing to LabMD that the 1718 File had been found on a peer-to-peer network and sending LabMD a Tiversa Incident Response Services Agreement describing Tiversa's proposed fee schedule, payment terms, and services that would be provided. These contacts continued from mid-May through mid-July 2008. In these communications, Tiversa represented that Tiversa had "continued to see individuals [on peer-to-peer networks] searching for and downloading copies" of the 1718 File. (RX0050; RX0051; RX0052; RX0053; RX0054; RX0055; RX0056; RX0057; RX0058; RX0059; CX0021; *see also* Daugherty, Tr. 979-993).

129. Tiversa's representations in its communications with LabMD (F. 128) that the 1718 File was being searched for on peer-to-peer networks, and that the 1718 File had spread across peer-to-peer networks, were not true. These assertions were the "usual sales pitch" to encourage the purchase of remediation services from Tiversa. (Wallace, Tr. 1443).

130. On July 22, 2008, LabMD instructed Tiversa to direct any further communications to LabMD's lawyer. Thereafter, Tiversa ceased to press LabMD to purchase its services. (RX0059; Daugherty, Tr. 988-990).

c. Tiversa's role as source for FTC investigation

131. The FTC offered testimony concerning peer-to-peer file-sharing technology at a July 2007 hearing conducted by the House of Representatives' Committee on Oversight and Government Reform regarding peer-to-peer file-sharing technology ("2007 Congressional Hearing"). (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues)).

132. Tiversa's Mr. Boback gave testimony at the 2007 Congressional Hearing regarding peer-to-peer file-sharing technology. (Wallace Tr. 1341-1342, 1347).

133. The FTC and Tiversa began communicating approximately two months after the 2007 Congressional Hearing. These communications were as frequent as weekly during some periods. The subject matter of these communications was information available on peer-to-peer networks. (Wallace, Tr. 1346-1347, 1350).

[21] "Browse host" is the ability for one LimeWire user to view all the files another LimeWire user has made available to share. (RX0533 (Fisk Expert Report at 16)).

134. In the fall or winter of 2007, representatives of the FTC visited Tiversa's facility in Pennsylvania. Following that meeting, the FTC began requesting that Tiversa provide information to the FTC. (Wallace, Tr. 1350-1351).

135. Tiversa did not want the FTC to issue a formal request for information, such as a Civil Investigative Demand ("CID"), directly to Tiversa because Tiversa had been in talks regarding a possible acquisition and Mr. Boback did not want Tiversa to be "in the middle of a civil investigative demand." Mr. Boback wanted the CID to be issued to a third party to "separate" the CID from Tiversa, "to try to create some distance" from Tiversa. (CX0703 (Boback, Dep. at 142-143); Wallace, Tr. 1351-1353, 1362).

136. The Privacy Institute was created for the purpose of receiving the CID from the FTC. The Privacy Institute did not exist previously. (RX0541 (Boback Trial Dep. at 38-40; 42-44); Wallace, Tr. 1353).

137. In 2009, in order to obtain Tiversa's information and documents, the FTC issued a CID to The Privacy Institute ("FTC CID"), and not to Tiversa, which was the actual target of the CID. (Kaufman, Tr. 1114; RX0525 (Kaufman, Dep. at 11-20) ("There was a request from Tiversa that we issue the CID to The Privacy Institute, and that is the entity that received the CID from the FTC.").

138. In response to the FTC CID to The Privacy Institute (F. 137), the FTC received the 1718 File and other evidence that "is germane to th[is] case." (CX0697 (*in camera*); Kaufman, Tr. 1114; RX0525 (Kaufman, Dep. at 11-20); *see also* RX0526 (Complaint Counsel's Amended Response to LabMD, Inc.'s First Set of Requests for Admission, Response No. 20 (admitting that as part of Complaint Counsel's Part II investigation of LabMD, the FTC issued a CID to The Privacy Institute and received the 1718 File)).

139. Mr. Wallace assisted in responding to the FTC CID (F. 137) by composing a spreadsheet of names of companies whose information exposure met a threshold of exposing 100 individuals' personal information. He also collected the associated files, which were burned to a computer disc. (Wallace, Tr. 1353-1354).

140. The spreadsheet provided in response to the FTC CID (F. 137) was derived from Tiversa's list of IRC's, *i.e.*, companies that Tiversa had targeted to try to sell Tiversa's remediation services. (F. 113; Wallace, Tr. 1358-1359, 1452-1453; *see* CX0307).

141. Mr. Boback directed Mr. Wallace to "make sure [LabMD is] at the top of the list" being provided to the FTC pursuant to the FTC CID. (Wallace, Tr. 1365).

142. The list of names Tiversa provided to the FTC in response to the FTC CID (F. 137) includes LabMD and identifies LabMD as the "data owner/leaker" of a file identified as "insuranceaging_6.05.071.pdf". (CX0307; Wallace, Tr. 1394).

143. The list of names Tiversa provided to the FTC in response to the FTC CID (F. 137) contained names that did not meet the 100 person exposure threshold described in F. 139.

These names were placed on the list at Mr. Boback's direction in order to get Tiversa "more bang for the buck," *i.e.*, in the hope that once the company was contacted by the FTC, the company would then buy Tiversa's services out of fear of an enforcement action. (Wallace, Tr. 1362-1363).

144. The list of names provided by Tiversa to the FTC in response to the FTC CID (F. 137), at Mr. Boback's direction, was "scrubbed" of names of existing or prospective Tiversa clients that otherwise met the 100 person exposure threshold. (Wallace, Tr. 1363-1364).

145. In the fall of 2009, representatives of Tiversa, including Mr. Wallace and Mr. Boback, met with FTC staff, including a member of Complaint Counsel's trial team in this case, to discuss Tiversa's response to the FTC CID (F. 137). (Wallace, Tr. 1385-1386, 1452).

d. CX0019

146. On the return trip from Tiversa's meeting with FTC staff in 2009 (F. 145), based on statements of Mr. Boback, Mr. Wallace understood that Tiversa needed to increase the apparent "spread" of the files identified on the list provided to the FTC pursuant to the FTC CID; that Mr. Wallace was to search for the files again to see if they are available at other IP addresses in addition to the address provided on the list; and that if the files were not, in fact, available at any additional IP addresses, Mr. Wallace was to make it appear that the files were available at additional IP addresses. (Wallace, Tr. 1386-1388).

147. After Tiversa's meeting with FTC staff in 2009 (F. 145), Mr. Wallace searched Tiversa's Data Store to see if the LabMD insurance aging file had been "picked up" from the automatic searches being performed by Tiversa for its healthcare clients, and he determined that it had not been. (Wallace, Tr. 1388-1390).

148. CX0019 purports to show that Tiversa had downloaded the 1718 File from four IP addresses on particular dates and times. Mr. Wallace created CX0019, at Mr. Boback's direction, in 2013, near the time of Boback's deposition, to make it appear that the 1718 File had "spread" to IP addresses belonging to known identity thieves, and that the 1718 File had not been found at an Atlanta IP address, when, in fact, none of this is true. Mr. Boback specifically asked Mr. Wallace to include a San Diego IP address. (Wallace, Tr. 1368-1370, 1381, 1446-1447).

149. Although it was not true, Mr. Wallace included on CX0019 the IP address 173.16.83.112 as one of the IP addresses where the 1718 File had been found because that IP address belonged to an individual in Apache Junction, Arizona that Wallace believed to be an identity thief, based on data in Tiversa's Data Store indicating that the individual at that address possessed over 3,000 tax returns that he appeared to be selling. (Wallace, Tr. 1376-1377).

150. In order to appear to be providing a client with valuable information, Tiversa would create the appearance of a "spread" of a client's file. (F. 115, 117-119; Wallace, Tr. 1391).

151. It was common practice for Tiversa to create documents such as CX0019 to make it appear that a file had "spread" to various IP addresses. (Wallace, Tr. 1368-1369, 1390-1391).

152. Tiversa had approximately 20 IP addresses that it would use when making it appear as if files had been spread across the Internet, including to identity thieves. Some IP addresses were used more frequently than others. For example, Tiversa knew of IP addresses that had gone "dead" after law enforcement took action. If Tiversa claimed the 1718 File was found at one of these long-gone addresses, such as the IP address at Apache Junction (F.149), there would be no way to contradict Tiversa's claim. (Wallace, Tr. 1376-1377, 1445).

153. The 1718 File was never found at any of the four IP addresses listed on CX0019. (Wallace, Tr. 1370, 1383-1384).

154. To Mr. Wallace's knowledge, the originating disclosing source in Atlanta is the only location at which the 1718 File was ever located. (Wallace, Tr. 1443-1444).

4. Credibility Findings Concerning the 1718 File Incident

155. Based on Mr. Wallace's forthrightness in response to questioning, and his overall demeanor observed during his questioning, Mr. Wallace is a credible witness.

156. Tiversa "has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations." (Dissenting Statement of Commissioner J. Thomas Rosch re FTC File No. 1023099 (June 21, 2012) at 1, *at* https://www.ftc.gov/sites/default/files/documents/petitions-quash/labmd-inc./1023099-labmd-full-commission-review-jtr-dissent.pdf; *see also e.g.*, F. 100, 108-114, 121, 126, 128).

157. Mr. Boback was motivated to retaliate against LabMD for LabMD's refusal to purchase remediation services from Tiversa, including by making the disclosure of the 1718 File appear widespread and dangerous. (F. 115-118, 126, 128-130, 148-154).

158. Mr. Boback's motive to retaliate against LabMD for refusing to purchase remediation services from Tiversa (F. 157) resulted in Tiversa's decision to include LabMD in the information provided to the FTC in response to the FTC CID (F. 137) and in the creation of CX0019. (F. 141-144, 146-149).

159. CX0019 is not credible or reliable evidence to show that the 1718 File spread on any peer-to-peer network. (F. 156-158).

160. Because of Mr. Boback's biased motive, Mr. Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent. (F. 156-159).

161. Mr. Boback has previously asserted that Tiversa found other files that it had not found. (F. 162-163).

162. Mr. Wallace helped Mr. Boback prepare for his testimony before the 2007 Congressional Hearing by giving Boback documents that Wallace had found on the Internet via peer-to-peer sharing from a time period that was before Tiversa had hired Wallace. Mr. Boback testified at the 2007 Congressional Hearing that Tiversa's system had found those documents, when in fact, Mr. Wallace, and not Tiversa or someone using Tiversa's system, had done so. (Wallace, Tr. 1432-1434).

163. There were "multiple times" when Mr. Boback would make statements that a company's documents had spread all over the Internet and then create the appearance that information was found in locations where it never existed. (Wallace, Tr. 1453-1454, 1457-1458) (testifying to a highly publicized instance as one example).

164. In 2014, the Chairman of the United States House Oversight and Government Affairs Committee ("OGR") commenced an investigation of Tiversa regarding its involvement with government agencies. The investigation continued over a period of months and included investigation into Tiversa's relationship with the FTC. (JX0003; RX0542 (June 11, 2014 OGR Letter from Issa to Ramirez); RX0543 (December 1, 2014 OGR Letter from Issa to Ramirez)).

165. The OGR staff report regarding the investigation referred in F. 164 concluded, *inter alia*, that Tiversa and Mr. Boback provided incomplete, inconsistent, and/or conflicting information to the FTC in this matter. (RX0644).

166. Having observed Mr. Boback's June 7, 2014 video deposition (RX0541 (Boback Trial Dep.); Tr. 1268-1269), taken by Respondent for purposes of trial testimony, Mr. Boback was evasive and lacked forthrightness in response to questioning.

167. Based on F. 155-166, and observation of Mr. Boback's overall demeanor during the June 7, 2014 video deposition (RX0541 (Boback Trial Dep.)), Mr. Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent.

168. Mr. Wallace's testimony, including without limitation regarding CX0019, is credited over any contrary testimony or other evidence provided by Boback or Tiversa. (F. 155-167).

5. Professor Eric Johnson

169. In February 2009, Professor Eric Johnson, while with Dartmouth College ("Dartmouth"), authored an article titled, "Data Hemorrhages in the Health-Care Sector." The article addresses data breaches and inadvertent disclosures of information by healthcare providers (the "Johnson Article"). (CX0382; Johnson, Tr. 753, 757).

170. Tiversa was a research partner for the Johnson Article, and assisted Professor Johnson in his research for the Johnson Article. (Johnson, Tr. 753-755).

171. The Johnson Article represents that the 1718 File was found as a result of Professor Johnson's research. (CX0382 at 11).

172. Tiversa's role in the research was to conduct searches for Professor Johnson and to forward files to him for further analysis. All the files examined in Professor Johnson's research for the Johnson Article were provided to him by Tiversa. (Johnson, Tr. 758-759, 793-794).

173. The first phase of the research, conducted in the first two weeks of January 2008, used a set of search terms, or "digital signature," related to the top ten publicly traded healthcare companies, as well as "generic" healthcare-related terms. The first phase of Professor Johnson's research did not uncover the 1718 File. (Johnson, Tr. 758-759, 765-766, 776-777, 780).

174. The second phase of Professor Johnson's research took place over a six-month period in the spring of 2008. It was Professor Johnson's "understanding" that files provided by Tiversa in the second phase of the research were files that Tiversa discovered by searching "host" locations found in the first phase of the research, or were files that Tiversa had otherwise discovered on its own. (Johnson, Tr. 762-763).

175. Although Professor Johnson understood that Tiversa had found the 1718 File, he had no knowledge of what search term was used to find the 1718 File. (Johnson, Tr. 764-765).

176. Tiversa employee Mr. Chris Gormley was Professor Johnson's main contact at Tiversa to discuss the research and progress of the Johnson Article. (Johnson, Tr. 770-771).

177. In an email to Mr. Gormley dated April 29, 2008, Professor Johnson stated that it was going "well on the medical files. We are working on the report right now. We turned up some interesting stuff – not as rich as the banks, but I guess that could be expected. Any chance you could share a couple of your recent medical finds that we could use to spice up the report? You told me about the one database you found that could really boost the impact of the report." (RX0483 at 1-2).

178. The 1718 File was one of many files that Tiversa provided to Professor Johnson. Despite persistent questioning, Professor Johnson did not provide a clear response as to: (1) whether Tiversa provided the 1718 File as a product of Professor Johnson's research parameters, including the "host" browsing second phase of Professor Johnson's research, as asserted in the Johnson Article; or (2) whether Tiversa provided the 1718 File in response to Professor Johnson's April 2008 request (F. 177) that Tiversa provide a "recent medical find" to "spice up" the Johnson Article. (Johnson, Tr. 774-777, 779-780; CX0382 at 11 (stating that the 1718 File was discovered in the second phase through

examining shared files on hosts where other "dangerous" data had been found); CX0483 at 2).

179. While Professor Johnson was confident that the 1718 File was not found in the first phase of his research, Professor Johnson either does not know, or was unwilling to say, whether the 1718 File was discovered as a result of his search protocol for the second phase of the research, notwithstanding the contrary representation in the Johnson Article. (*See* F. 173-175, 178; Johnson, Tr. 777-780).

180. An FTC attorney contacted Professor Johnson in February 2009, and asked for a copy of the Johnson Article, and Professor Johnson complied by sending a copy. (RX0403; Johnson, Tr. 784).

181. Professor Johnson did not provide the 1718 File to the FTC, and did not share files containing sensitive information with anyone. (Johnson, Tr. 785, 794).

E. THE SACRAMENTO INCIDENT

1. Sacramento Police Department's Discovery of LabMD Documents

182. On October 5, 2012, the Sacramento California Police Department (the "SPD") found 40 LabMD "day sheets," (F. 199) (hereafter, the "Day Sheets"), 9 copied checks, and 1 money order made payable to LabMD in a house in Sacramento, California (collectively, the "Sacramento Documents"). (Joint Stipulations of Fact, JX0001-A at 4; CX0087, *in camera* (LabMD Day Sheets); CX0088, *in camera* (LabMD Copied Checks at 1-10); CX0720 (Jestes, Dep. at 17-18, 22-23, 33-37)). This event is referred to herein as the "Sacramento Incident."

183. The Day Sheets found by the SPD on October 5, 2012 contain the following Personal Information of approximately 600 consumers: names and nine digit chart numbers that appear to be SSNs. (CX0720 (Jestes, Dep. at 35-37); CX0087, *in camera* (LabMD Day Sheets); RRCCFF 1724).

184. The dates of the Day Sheets contained in CX0087 range from June 2007 to March 2009, with 28 from various months in the year 2008, 10 from various months in 2007, and 2 from March 2009. (CX0087, *in camera* (LabMD Day Sheets)).

185. The nine copied checks found by the SPD on October 5, 2012 contain the following Personal Information of nine consumers: names, addresses (for all but one), and bank account numbers. The money order does not contain any Personal Information. (CX0088 *in camera*, (LabMD Copied Checks at 1-10)).

186. The dates of the nine copied checks found by the SPD on October 5, 2012 range from May 2007 to March 2009. (CX0088, *in camera* (LabMD Copied Checks at 1-9) (4 checks from 2007; 4 checks from 2008; 1 check from 2009)).

187. The date of the one money order found by the SPD on October 5, 2012 is August 21, 2008. (CX0088, *in camera* (LabMD Copied Checks at 10)).

188. Detective Karina Jestes of the SPD participated in an investigation of 5661 Wilkinson Street in Sacramento, California ("5661 Wilkinson"), initiated on October 5, 2012, along with three other officers. (CX0720 (Jestes, Dep. at 17-18)).

189. The SPD investigation concerned a woman whose utility bill had been compromised and who was then receiving an additional utility bill for an address at 5661 Wilkinson, to which she had no connection. (CX0720 (Jestes, Dep. at 17-18)).

190. Detective Jestes went to 5661 Wilkinson, entered the property, and executed a search. (CX0720 (Jestes, Dep. at 17-19)).

191. Detective Jestes concluded that the search of 5661 Wilkinson revealed evidence of utility billing theft, evidence that the occupants of the home were using someone else's name for the gas utility bill, narcotics paraphernalia, narcotics, and several additional items that, Detective Jestes believed, showed that identity theft was occurring at the house. (CX0720 (Jestes Dep. at 19-20)).

192. The search of 5661 Wilkinson also uncovered the Sacramento Documents, described in F. 182-187. (Joint Stipulations of Fact, JX0001-A at 4; CX0720 (Jestes, Dep. at 23)).

193. On October 5, 2012, Mr. Erick Garcia and Ms. Josie Maldonado were arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. (CX0720 (Jestes, Dep. at 25)).

194. Mr. Garcia and Ms. Maldonado pled *nolo contendere* to identity theft and were sentenced to probation and a sheriff's work project. (CX0720 (Jestes, Dep. at 43-45)).

195. The Day Sheets found by the SPD during the search of 5661 Wilkinson on October 5, 2012 were seized by the SPD and booked into evidence. (CX0720 (Jestes, Dep. at 30-31)).

196. The copies of checks and the canceled money order found by the SPD during the search of 5661 Wilkinson on October 5, 2012 were seized by the SPD and booked into evidence. (CX0720 (Jestes, Dep. at 31-32)).

2. Connection between the Sacramento Documents and LabMD's Computer Network

197. The Sacramento Documents were found in paper form, not in electronic form. (CX0720 (Jestes, Dep. at 58)).

198. As part of its consumer billing process, LabMD produced reports called day sheet transaction detail reports, referred to as "day sheets." (CX0715-A (Gilbreth, Dep. at 42); *see, e.g.*, CX0087, *in camera*).

199. Day sheets are reports that were created, accessed, and printed electronically through LabMD's billing application, Lytec, to ensure payment had been received and posted. (CX0733 (Boyle, IHT at 33); CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Former LabMD Employee], Dep. at 59-60)).

200. LabMD's billing department used computers to create day sheets of payments received from consumers, which may include consumers' names; SSNs; and methods, amounts, and dates of payments. (Answer ¶ 9(b); CX0715-A (Gilbreth, Dep. at 37-38, 46-49)).

201. Day sheets could include billing date; provider number; place of service; diagnosis code, which is a standardized code that identifies the symptoms leading to the procedure being performed; payment code; payment amount; charges; credits; and adjustments. (CX0714-A ([Former LabMD Employee], Dep. at 62-63); CX0715-A (Gilbreth, Dep. at 48-49); *e.g.*, CX0087, *in camera*).

202. Copies of patient checks were attached to day sheets. (CX0715-A (Gilbreth, Dep. at 50-51)).

203. Day sheets were created electronically but were not saved electronically. Day sheets were then printed almost every day. Once the day sheets were printed, "there is no electronic record in the system." (CX0733 (Boyle, IHT at 37-38); CX0715-A (Gilbreth, Dep. at 43); CX0714-A ([Former LabMD Employee], Dep. at 59-60)).

204. The printed day sheets were made part of batch reports. If a batch report did not balance, then the day sheet was shredded and a new day sheet was created. Only balanced day sheets were retained. (CX0714-A ([Former LabMD Employee]), Dep. at 61-62).

205. Day sheets could be printed by any of LabMD's billing employees who posted payments or by a LabMD billing manager. (CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Former LabMD Employee], Dep. at 64-65)).

206. Day sheets were stored in paper files at LabMD. (CX0733 (Boyle, IHT at 33-39); CX0710-A (Daugherty, LabMD Designee, Dep. at 60); CX0715-A (Gilbreth, Dep. at 43-45); CX0714-A ([Former LabMD Employee], Dep. at 58-61)).

207. After day sheets were generated by LabMD through the Lytec system, although LabMD billing employees had the option to save or to print off day sheets, LabMD billing employees did not save them. (CX0714-A ([Former LabMD Employee], Dep. at 60-61 ("I don't know of anyone who actually saved them. . . . "I never saved [them]."));
CX0715-A (Gilbreth, Dep. at 43 (day sheet reports were not created in an electronic format such as an electronic file)).

208. Beginning in or around January 2013, LabMD began to electronically scan some of its documents for a medical records archiving project. This project began with archiving old insurance documents, such as Explanation of Benefits documents. The archiving project, which was ongoing, has also included scanning of some retained day sheet printouts and check copies. (CX0716 (Harris Dep. at 25-26); CX0733 (Boyle, IHT at 37, 46-47)).

3. Follow up to Discovery of the Sacramento Documents

209. After finding the Sacramento Documents, Detective Jestes performed an Internet search and learned that the FTC was investigating LabMD. Approximately one week after the October 5, 2012 discovery of the Sacramento Documents, Detective Jestes contacted the FTC regarding the Sacramento Documents. (CX0720 (Jestes, Dep. at 60-62)).

210. In December 2012, the SPD provided the Sacramento Documents to the FTC. The SPD made the determination not to return the Sacramento Documents to LabMD based on the FTC's investigation of LabMD. (CX0720 (Jestes, Dep. at 60-61)).

211. On January 30, 2013, the FTC notified LabMD that the FTC had the Sacramento Documents. (CX0227; Daughtery, Tr. 1013-1014).

212. On March 27 or 28, 2013, LabMD sent 682 letters to the consumers named in the Sacramento Documents notifying them of the Sacramento Incident, describing steps such as registering a fraud alert with credit bureaus, offering one year of free credit monitoring services, and inviting consumers to contact LabMD with questions or concerns. (CX0710-A (Daugherty, LabMD Designee, Dep. at 63, 68-69); CX0709 (Daugherty, Dep. at 120); CX0227).

4. Lack of Foundation for Admission of CX0451

213. Mr. Kevin Wilmer is an investigator with the FTC. (Wilmer, Tr. 331).

214. CLEAR (Consolidated Lead Evaluation and Reporting) is an investigative software database program, provided by Thompson Reuters Corporation (Thompson Reuters), that is used by investigators at the FTC to obtain information on individuals and corporations. Mr. Wilmer's "understanding," based on his training and experience with the CLEAR database, is that the information contained in the CLEAR database is an aggregation of information obtained from a variety of sources, including credit bureau information, utility information, information from civil judgments and criminal convictions, and other forms of publicly and privately available information. (Wilmer, Tr. 335, 359, 362, 364).

215. Mr. Wilmer was provided with an electronic copy of CX0085, which he was told consisted of copies of the Sacramento Documents (F. 182). (Wilmer, Tr. 338-339).

216. The first four pages of CX0085 are copies of the checks and a canceled money order found by the SPD during the search of 5661 Wilkinson on October 5, 2012 that comprise CX0088. Pages 5 through 44 of CX0085 are copies of the Day Sheets found by the SPD

during the search of 5661 Wilkinson on October 5, 2012 that comprise CX0087. (CX0085, *in camera* (LabMD Day Sheets and Copied Checks).

217. Mr. Wilmer concluded, but did not confirm, that the nine digit numbers in pages 5 through 44 of CX0085 represented Social Security numbers. (Wilmer, Tr. 340).

218. Mr. Wilmer was asked by Complaint Counsel to determine whether Social Security numbers in pages 5 through 44 of CX0085 had been used by people with different names. He was not asked to confirm that the nine digit numbers appearing on CX0085 are Social Security numbers corresponding to the names that are listed on CX0085. (Wilmer, Tr. 341-342).

219. To perform the task set forth in F. 218, Mr. Wilmer issued a "query" to the CLEAR database. Specifically, Mr. Wilmer copied each number that he believed to be a Social Security number from CX0085 and pasted the number onto a CLEAR-provided spreadsheet. He then submitted the spreadsheet with a request that CLEAR use its "batching" function to query the CLEAR database to determine who used that apparent Social Security number and return the information to him. (Wilmer, Tr. 342-345, 359-360).

220. In response to Mr. Wilmer's CLEAR database query, described in F. 219, CLEAR returned a spreadsheet containing the nine digit numbers that Mr. Wilmer had entered, and CLEAR's data, drawn from its various sources, as to the names of people who used those numbers. The CLEAR spreadsheet also provided in some instances a date of birth, date of death, gender, home address and the first or last time a number was used. (Wilmer, Tr. 345-346, 361, 364).

221. Mr. Wilmer identified a document, marked for identification as CX0451, as the results returned to him by Thompson Reuters in response to his CLEAR database query, to which Mr. Wilmer added certain color coding to differentiate various names. (Wilmer, Tr. 350, 359).

222. Mr. Wilmer does not know whether the nine digit numbers he copied from CX0085 and entered into his CLEAR database query as apparent Social Security numbers actually belonged to the associated names on CX0085. (Wilmer, Tr. 358).

223. CX0451 does not indicate which individual associated with a Social Security number is the true owner of the number, if any. CLEAR only indicates that an individual is associated with a Social Security number. (Wilmer, Tr. 363-364).

224. Mr. Wilmer did not ask CLEAR to identify the source(s) of the data that CLEAR used to populate the CLEAR spreadsheet, although he could have received this information if he asked, because that was not part of his assignment. (Wilmer, Tr. 365).

225. Mr. Wilmer does not know, and did not ask CLEAR, whether any of the numbers reported by CLEAR as a Social Security number associated with an individual had

stemmed from bad keystrokes on the part of a reporting source such as a bank. (Wilmer, Tr. 366).

226. Mr. Wilmer does not know if some of the people listed on CX0085 had knowingly and willingly shared their personal information for others to use, or whether they had family members who may have taken their personal information without consent. Mr. Wilmer was not asked to determine these matters, and was not asked to and did not contact any of the individuals listed on CX0085. (Wilmer, Tr. 367-369).

227. Based on the failure to demonstrate the authenticity or reliability of the data returned by the CLEAR database, which is contained in proffered CX0451, the document cannot properly support any factual finding or any valid conclusion in this case. (*See* F. 217-226).

F. IDENTITY THEFT HARM

228. "Identity theft" refers to the use of another person's identity without his or her permission. This includes using another person's personal identifiers to impersonate that person. (CX0742 (Kam Expert Report at 10); Kam, Tr. 394).

229. "Identity fraud" refers to the unauthorized use of another person's information to achieve illicit financial gain. Types of identity fraud are "new account fraud," "existing non-card fraud," and "existing card fraud." (CX0742 (Kam Expert Report at 10); CX0741 (Van Dyke Expert Report at 3)).

230. "New account fraud" ("NAF") is identity fraud perpetrated through the use of another person's personally identifiable information to open new, fraudulent accounts. (CX0741 (Van Dyke Expert Report at 3)).

231. "Existing non-card fraud" ("ENCF") is identity fraud perpetrated through the use of existing checking or savings accounts or existing loans, insurance, telephone, and utilities accounts. (CX0741 (Van Dyke Expert Report at 3)).

232. "Existing card fraud" ("ECF") is identity fraud perpetrated through use of existing credit or debit cards and/or their account numbers. (CX0741 (Van Dyke Expert Report at 3)).

233. "Medical identity theft," also known as "medical identity fraud," is the unauthorized use of a third party's personally identifiable information to obtain medical products or services, including but not limited to: office visits and consultations, medical operations, and prescriptions. Medical identity theft may also include attempts to fraudulently bill health insurance providers. (CX0741 (Van Dyke Expert Report at 3); CX0742 (Kam Expert Report at 11-12); Kam, Tr. 395).

234. A "data breach" refers to the unauthorized disclosure of personally identifying information. (Van Dyke, Tr. 589; Kam, Tr. 378).

235. As a matter of common usage, the generic term "identity theft" may include "identity fraud" (with its subsets, NAF, ENCF, ECF, and medical identity theft). (Van Dyke, Tr. 577-579; CX0741 (Van Dyke Expert Report at 3)).

236. Identity theft and identity fraud are distinguishable from a "data breach," in that a data breach refers only to the unauthorized exposure of personal information, while identity theft and identity fraud refer to the improper use of personal information. (F. 228-229, 234).

237. Complaint Counsel's proffered expert on computer security, Dr. Raquel Hill (F. 4-5), acknowledged that she did not have an opinion with regard to the likelihood of consumer harm. Dr. Hill was instructed to "assume" that identity theft harm could occur if the information contained on LabMD's network was exposed. Dr. Hill further assumed, in assuming such harm could occur, that such harm was likely. (Hill, Tr. 216-219; CX0740 (Hill Expert Report at 20 ¶ 49)).

238. Complaint Counsel's proffered expert on the likelihood of consumer harm in this case, Mr. Rick Kam (F. 9-11) used the following four factors to examine "the likely risk of harm to consumers from unauthorized disclosure" of Personal Information: (1) the nature and extent of the sensitive Personal Information exposed; (2) the unauthorized person who obtained information or to whom the disclosure was made, to determine whether the person possessing the information presents a low risk of misuse, or a higher risk of misuse, such as an identity thief; (3) whether the sensitive Personal Information was actually acquired or viewed; and (4) the extent to which the risk from the exposure has been mitigated, including whether or not "the data is still available for others to misuse." (Kam, Tr. 404-406; CX0742 (Kam Expert Report at 17-18)).

239. Mr. Kam applied the four factor risk assessment test referenced in F. 238 to determine the likelihood of harm from the exposure of the 1718 File. (CX0742 (Kam Expert Report at 18-19)).

240. In applying the second and third factors of the four factor risk assessment test (F. 238) to determine the likelihood of identity theft harm from the disclosure of the 1718 File, Mr. Kam relied upon the discredited deposition testimony of Mr. Boback (F. 167) that the 1718 File was found at four IP addresses, along with unrelated sensitive consumer information that could be used to commit identity theft, and that law enforcement had apprehended someone suspected of identity theft of fraud using one of those IP addresses. (CX0742 (Kam Expert Report at 19); Kam, Tr. 409-410).

241. In applying the second and third factors of the four factor risk assessment test (F. 238) to determine the likelihood of identity theft harm from the disclosure of the 1718 File, Mr. Kam relied upon the discredited deposition testimony of Mr. Boback (F. 167) that the 1718 File had been found at four IP addresses on four different dates and had also been found by Tiversa just before Mr. Boback provided deposition testimony in November 2013. (CX0742 (Kam Expert Report at 19); Kam, Tr. 409-410).

242. In Mr. Kam's experience, in every data breach, some victim has come forward. Mr. Kam acknowledged that no evidence has been presented of any individual listed in the Sacramento Documents or in the 1718 File having come forward to report identity theft harm. (Kam, Tr. 532-533).

243. Mr. Kam was unaware of any actual victims of identity theft or fraud of any individuals listed on the 1718 File. (Kam, Tr. 507).

244. For the purposes of his analysis, Mr. Kam "assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks." (CX0742 (Kam Expert Report at 5)).

245. Mr. Kam is not an expert in computer network security and did not analyze any of LabMD's specific practices with respect to LabMD's computer networks or assess the probability that LabMD's computer networks will be breached in the future. (Kam, Tr. 518).

246. Mr. Kam based his opinion on the likelihood of medical identity theft harm primarily on the 2013 Survey on Medical Identity Theft by Ponemon Institute ("2013 Ponemon Survey"). (CX0742 (Kam Expert Report at 15, 19-20); Kam, Tr. 423).

247. The 2013 Ponemon Survey, conducted in September 2013, had a response rate of only 1.8 %, which the 2013 Ponemon Survey acknowledged, and which, Mr. Kam agreed, creates a non-response bias, *i.e.*, a failure to take into account that those who were surveyed but did not respond might have a different answer to the question. (Kam, Tr. 540-541; RX0528 (2013 Ponemon Survey at 31)).

248. The 2013 Ponemon Survey's sampling frame (the source from which a sample is drawn) contained individuals who were prescreened from a larger sample on the basis of their identity theft or identity fraud experience. The 2013 Ponemon Survey acknowledged, and Mr. Kam agreed, that this resulted in a sampling frame bias. (RX0528 (2013 Ponemon Survey at 28, 32); Kam, Tr. 541).

249. The 2013 Ponemon Survey compensated respondents to complete the survey within a set period of time, which the 2013 Ponemon Survey acknowledged was an inherent limitation to its survey research. (RX0528 (2013 Ponemon Survey at 32); *see also* Kam, Tr. 541).

250. The 2013 Ponemon Survey stated: "[m]any cases of medical identity theft reported in this study result from the sharing of personal identification with family and friends. In some cases, family members take the victim's personal credentials without consent. Rarely does it occur from data breaches, malicious insiders, an identity thief or loss of medical credentials." (RX0528 (2013 Ponemon Survey at 27)).

251. Mr. Kam acknowledged that medical identity theft rarely occurs from data breaches or the acts of an identity thief and acknowledged that most occurrences of medical identity

theft were from someone knowingly sharing their personal information or medical credentials and from instances where a family member took another family member's personal information or medical credentials without consent. (Kam, Tr. 486-487).

252. Complaint Counsel's second proffered expert on the likelihood of consumer harm in this case, Mr. James Van Dyke (F. 12-15) based his analysis principally on identity theft statistics derived from the Javelin 2013 Identity Fraud Survey ("2013 Javelin Survey"). The 2013 Javelin Survey was conducted in October 2013 among 5,634 adults in the United States. Javelin's 2014 Identity Fraud Report ("2014 Javelin Report") is based on the results of the 2013 Javelin Identity Fraud Survey. The Javelin Identity Theft Survey is conducted annually. (CX0741 (Van Dyke Expert Report at 2-4, and Attachment 1); Van Dyke, Tr. 583, 602-604).

253. Mr. Van Dyke selected the 2013 Javelin Survey and 2014 Javelin Report to support his opinions and calculations of likely identity theft harm from the exposure of the 1718 File because of the discredited deposition testimony of Mr. Boback in November 2013 (F. 167) that Tiversa had located the 1718 File on peer-to-peer networks on IP addresses from four locations other than LabMD. (CX0741 (Van Dyke Expert Report at 6-8); Van Dyke, Tr. 668-669).

254. In connection with Javelin Research, Mr. Van Dyke has occasionally been provided with a list of names and asked to conduct a survey from among those individuals. (Van Dyke, Tr. 730).

255. Mr. Van Dyke did not conduct a survey of the 9,300 consumers listed on the 1718 File. (Van Dyke, Tr. 690, 726; *see also* CX0741 (Van Dyke Expert Report)).

256. Mr. Van Dyke did not conduct a survey of the 600 consumers listed in the Sacramento Documents. (*See* Van Dyke, Tr. 574-741; CX0741 (Van Dyke Expert Report)).

257. For the purposes of his analysis, Mr. Van Dyke "assumed that LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks" and that, therefore, all individuals whose information is maintained on LabMD's computer network are "at risk" of "exposure to a likelihood" of identity fraud and medical identity fraud. Mr. Van Dyke did not do any independent analysis of LabMD's network security. (CX0741 (Van Dyke Expert Report at 2, 13); Van Dyke, Tr. 695-696).

258. Mr. Van Dyke did not, and was unable to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose personally identifiable information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except as to those that were listed on the 1718 File or in the Sacramento Documents. (Van Dyke, Tr. 631; *see also* Van Dyke, Tr. 610).

III. ANALYSIS

A. BURDEN OF PROOF

The parties' burdens of proof are governed by Rule 3.43(a) of the Federal Trade Commission's ("FTC" or "Commission") Rules of Practice for Adjudicative Proceedings ("Rules"), Section 556(d) of the Administrative Procedure Act ("APA"), and case law. Pursuant to Commission Rule 3.43(a), "[c]ounsel representing the Commission . . . shall have the burden of proof, but the proponent of any factual proposition shall be required to sustain the burden of proof with respect thereto." 16 C.F.R. § 3.43(a). Under the APA, "[e]xcept as otherwise provided by statute, the proponent of a rule or order has the burden of proof." 5 U.S.C. § 556(d).

It is well established that the preponderance of the evidence standard governs FTC enforcement actions. *In re Rambus, Inc.*, 2006 FTC LEXIS 101, at *45 (Aug. 20, 2006); *In re POM Wonderful LLC*, 2012 FTC LEXIS 106, at *463-65 (May 17, 2012) (initial decision); *In re Adventist Health System/West*, 117 F.T.C. 224, 1994 FTC LEXIS 54, at *28 (Apr. 1, 1994) ("Each element of the case must be established by a preponderance of the evidence . . ."). The Supreme Court has held that Section 7(c) of the APA, which is applicable to administrative adjudicatory proceedings unless otherwise provided by statute, establishes "a standard of proof and . . . the standard adopted is the traditional preponderance-of-the evidence standard." *Steadman v. SEC*, 450 U.S. 91, 95-102 (1981).

Section 5(n) of the Federal Trade Commission Act ("FTC Act") requires that FTC Complaint Counsel ("Complaint Counsel") prove, *inter alia*, that challenged conduct "causes or is *likely to cause* substantial injury to consumers." 15 U.S.C. § 45(n) (emphasis added). Respondent argues that, because Section 5(n) uses the phrase "likely to cause," Complaint Counsel has the burden of proving the likelihood of substantial consumer injury in this case by clear and convincing evidence. This argument contradicts clearly established law, stated above, and Respondent's own stipulations in this case. *See* Joint Stipulations of Fact, JX0001-A at 2-3 ("The standard of proof is preponderance of the evidence."). None of the authorities cited by Respondent suggests that the term "likely" means that clear and convincing evidence is required in this case. *E.g., Colorado v. New Mexico*, 467 U.S. 310, 315-17 (1984) (applying heightened

standard of proof based on "the unique interests involved in water rights disputes between sovereigns," not because any statute involved required showing that any event was "likely"). Accordingly, Complaint Counsel has the burden of proving each factual issue supporting its claims against Respondent in this case by a preponderance of credible evidence.

B. JURISDICTION

Section 5 of the FTC Act grants the FTC the authority over "unfair or deceptive acts or practices in or affecting commerce" by "persons, partnerships, or corporations . . . ." 15 U.S.C. § 45(a)(1)-(2) (2012).[22] Respondent LabMD, Inc. ("Respondent" or "LabMD") is a privately held Georgia corporation, incorporated in 1996 by Mr. Michael J. Daugherty. F. 24. It is undisputed that Respondent is a corporation. Complaint ¶ 1; Answer ¶ 1. From at least 2001 through approximately January 2014, LabMD was in the business of conducting clinical laboratory tests on urological specimen samples and reporting test results to its physician clients. F. 26. Respondent stipulates that the acts and practices alleged in the Complaint are "in or affecting commerce." F. 30; *see* also F. 28-29.

In its order denying Respondent's November 12, 2013 Motion to Dismiss (*see* Section I.A.2. and footnote 1, *supra*), the Commission held that its jurisdiction over unfair practices extends to a "company's failure to implement reasonable and appropriate data security measures" and that it has jurisdiction over this case. *LabMD*, 2014 FTC LEXIS 2, at *3, *7. Believing the Commission's determination of its jurisdiction to be erroneous, Respondent reserves its jurisdictional challenge for its anticipated appeal to the federal court. RCL 146. Based on the foregoing, the issue of jurisdiction will not be revisited in this Initial Decision. *See In re North Carolina Bd. of Dental Examiners*, 2011 FTC LEXIS 137, at *180-82 (July 14, 2011) (declining to address respondent's state action immunity defense).

[22] Section 4 of the FTC Act defines "corporation," in part, as "any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members, and has shares of capital or capital stock or certificates of interest . . . ." 15 U.S.C. § 44.

C. LEGAL FRAMEWORK FOR DETERMINING UNFAIR CONDUCT

The Complaint alleges that (1) Respondent failed to provide "reasonable" security for Personal Information[23] on its computer networks, including because Respondent failed to have in place the data security practices specified in the Complaint at ¶¶ 10(a)-(g); and that (2) Respondent's alleged unreasonable data security "caused, or is likely to cause, substantial injury to consumers that is not reasonably avoidable, or offset by benefits to consumers or competition." Complaint ¶¶ 10, 22. Therefore, the Complaint charges, Respondent's alleged unreasonable data security "constitute[s] an unfair practice in violation of Section 5(a) of the FTC Act." Complaint ¶ 23. As authority for finding unfair conduct liability, Complaint Counsel relies on Section 5(n) of the FTC Act, which provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

Congress amended the FTC Act in 1994 to add Section 5(n). FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695. The intent of the amendment was not to expand, but to establish an outer limit to the Commission's authority to declare an act or practice unfair. *See* H.R. CONF. REP. 103-617 at 5, FTC Act Amendments of 1994, 1994 WL 385368, at *11-12 (July 21, 1994) (stating that new Section 5(n): "[a]mends section 5 of the Act to *limit* unfair acts or practices to those that: (1) cause or are likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or competition") (emphasis added). The three-part test in Section 5(n) was "intended to codify, as a *statutory limitation* on unfair acts or practices, the principles of the FTC's December 17, 1980, policy statement on unfairness, reaffirmed by a letter from the FTC dated March 5, 1982," in order to provide guidance and to

[23] The parties have stipulated that the term "Personal Information," as used by the parties, means: "Individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. F. 3.

prevent a future FTC from abandoning those principles. S. REP. 103-130, 1993 WL 322671, at *12 (Aug. 24, 1993) (emphasis added); *see* Letter from FTC to Senators Ford and Danforth (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *300 (Dec. 21, 1984) ("Policy Statement"); Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) ("1982 Policy Letter").

According to the Policy Statement, "[u]njustified consumer injury is the primary focus of the FTC Act." Policy Statement, 1984 FTC LEXIS 2, at *307. Moreover, the consumer injury must be substantial, and not "trivial or merely speculative." *Id*. In the 1982 Policy Letter, FTC Chairman Miller reiterated that the Commission's "concerns should be with substantial injuries; its resources should not be used for trivial or speculative harm." 1982 Policy Letter, *supra*. In adopting Section 5(n), Congress noted: "In most cases, substantial injury would involve monetary or economic harm or unwarranted health and safety risks." S. REP. 103-130, 1993 WL 322671, at *13. Furthermore, although a finding of unfair conduct can be based on "likely" future harm, "[u]nfairness cases usually involve actual and completed harms." *Int'l Harvester Co.*, 1984 FTC LEXIS 2, at *248; *accord In re Orkin Exterminating Co.*, 108 F.T.C. 263, 1986 FTC LEXIS 3, at *50 n.73 (Dec. 15, 1986).

Section 5(n) is clear that a finding of actual or likely substantial consumer injury, which is also not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition, is a legal precondition to finding a respondent liable for unfair conduct. *See LabMD*, 2014 FTC LEXIS 2, at *52 (Commission Order on Motion to Dismiss) (holding that determining Respondent's liability in this case requires determining whether the alleged "substantial injury" occurred, and "also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances"); *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 934-35 (N.D. Ill. 2008) ("[S]ubsection (n) . . . requires as a precondition to the FTC's authority to declare an act or practice to be 'unfair' that it be one that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"). *See also FTC v. Wyndham Worldwide Corp.*, 2015 U.S. App. LEXIS 14839, at **54 (3rd Cir. Aug. 24, 2015) (noting that "[t]he three requirements in § 45(n) may be necessary rather than

sufficient conditions" for finding unfair conduct). As explained below, the preponderance of the evidence in this case fails to show that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury. Accordingly, the Complaint must be dismissed, and it need not, and will not, be further determined whether or not Respondent's data security was, in fact, "unreasonable."[24]

D. CONSUMER HARM ANALYSIS

1. Terminology

As more fully detailed below, Complaint Counsel asserts that the "substantial consumer injury" at issue in this case consists of the monetary losses and other allegedly cognizable injuries that result from identity theft. Complaint Counsel also asserts intangible injuries that allegedly arise as a result of unauthorized disclosure of certain types of Personal Information through a data breach alone, apart from any resulting identity theft. "Identity theft" refers to the use of another person's identity without his or her permission. F. 228. "Identity fraud" refers to the unauthorized use of some portion of another person's information to achieve illicit financial gain. F. 229. Complaint Counsel uses the terms "identity theft" and "identity fraud" interchangeably. Identity theft and identity fraud are distinguishable from a "data breach," in that a data breach refers only to the unauthorized exposure of personal information, while identity theft and identity fraud refer to the improper use of personal information. F. 236.

As a matter of common usage, the generic term "identity theft" may include "identity fraud," new account fraud ("NAF"), existing non-card fraud ("ENCF"), existing card fraud ("ECF"), and medical identity theft. F. 229, 235. NAF is identity fraud perpetrated through the use of another person's personally identifiable information to open new, fraudulent accounts. F. 230. ENCF is identity fraud perpetrated through the use of existing checking or savings accounts or existing loans, insurance, telephone, and utilities accounts. F. 231. ECF is identity fraud perpetrated through the use of existing credit or debit cards and/or their account numbers. F. 232. Medical identity theft, also referred to as medical identity fraud, is the unauthorized use

[24] As detailed in Section II.C.1., *supra*, LabMD wound down its operations beginning in January 2014, and as of May 2014, LabMD's operations were limited to maintaining tissue samples and providing copies of prior test data to its physician clients only via facsimile. F. 36-39. Accordingly, references to LabMD's operations, including with respect to data security, are in the past tense.

of a third party's personally identifiable information to obtain medical products or services, including but not limited to: office visits and consultations, medical operations, and prescriptions. F. 233. Medical identity theft may also involve attempts to fraudulently bill insurance providers. F. 233.

Based on the foregoing, for ease of reference, unless the context indicates otherwise, "identity theft harm" as used in this analysis shall refer to injury arising from the misuse of personal information pursuant to identity theft, medical identity theft, and the other identity theft subtypes referred to above. Also, the terms "harm" and "injury" are used herein interchangeably, and, unless the context indicates otherwise, shall refer to all harms or injuries asserted by Complaint Counsel as meeting the "substantial injury" test set forth in Section 5(n).

2. Overview of Arguments on Substantial Consumer Injury

The Complaint alleges two "security incidents" in connection with Respondent's alleged unreasonable data security (hereafter "Security Incidents"). Complaint ¶¶ 17-21. As to the first Security Incident, the Complaint alleges that a "third party" informed LabMD that a June 2007 insurance aging report generated by LabMD was "available" on a peer-to-peer ("P2P") file-sharing network, through a file-sharing application called LimeWire. Complaint ¶ 17. This insurance aging report, consisting of 1,718 pages, is referred to herein as the "1718 File" and discussed in greater detail in Section III.D.5., *infra*. The second alleged Security Incident avers that, in October 2012, "more than 35 Day Sheets" and "a small number of copied checks" were found in the possession of individuals in Sacramento, California who subsequently pleaded "no contest" to identity theft charges. Complaint ¶ 21. The documents, referred to herein as the "Sacramento Documents," are discussed in greater detail in Section III.D.6, *infra*.

The Order on Post-Trial Briefs, issued on July 16, 2015, specifically directed the parties to address the issue of the substantial consumer injury requirement of Section 5(n) as follows:

> Complaint Counsel shall fully and clearly articulate, and Respondent shall fully and clearly reply to, Complaint Counsel's theory of "substantial injury" in this case, including, without limitation: (1) the specific nature of the substantial injury or injuries asserted; (2) whether such asserted substantial injuries constitute

> present or future injuries; and, (3) as applicable, an assessment of the risk and/or likelihood of the asserted substantial injuries.

In re LabMD, Inc., 2015 FTC LEXIS 178, at *8-9 (July 16, 2015).

Having reviewed and considered the totality of Complaint Counsel's post-trial filings, including Complaint Counsel Post-Trial Brief, Proposed Findings of Fact and Conclusions of Law, and replies to Respondent's post-trial filings, Complaint Counsel's argument appears to assert the following as meeting the "substantial injury" requirement in Section 5(n):

- Likely identity theft harm for consumers whose Personal Information was exposed in the 1718 File and the Sacramento Documents, including monetary losses from NAF, ECF, and ENCF, based on an "increased risk" that consumers whose information is exposed in a data breach will suffer identity theft harm;

- Likely medical identity theft harm for consumers whose Personal Information was exposed in the 1718 File,[25] including monetary losses due to fraudulently procured medical products and services, and health and safety risks;

- "Significant risk" of reputational harm, privacy harm, and/or other harms based on stigma or embarrassment, caused by the unauthorized exposure of asserted "sensitive medical information" in the 1718 File; and,

- "Risk" of harm to all consumers whose information is maintained on LabMD's computer network, which Complaint Counsel variously describes as the "risk," "increased risk," or "significant risk," that Respondent's computer network will suffer a future data breach, resulting in identity theft harm, medical identity theft harm, and/or other harm.

See, e.g., CCB 63-72; CCCL 27, 30, 33, 35-40; CCFF §§ 8.2, 8.3, 8.4. *See also* CX0741 (Van Dyke Expert Report); CX0742 (Kam Expert Report).

On the issue of substantial consumer injury, Respondent contends, in summary, that Complaint Counsel has failed to meet its burden of proving actual or likely consumer harm as a result of Respondent's alleged unreasonable data security. Respondent asserts that there is no evidence that any consumer has suffered any actual harm as a result of Respondent's alleged unreasonable data security, and that the evidence fails to show that any harm is probable in the

[25] Complaint Counsel's brief and proposed findings of fact do not address the likelihood of medical identity theft from the exposure of the Sacramento Documents. *See* CCB at 71-72; CCFF § 8.4. To the extent Complaint Counsel asserts that the exposure of the Sacramento Documents is likely to cause medical identity theft harm, as set forth below, the evidence fails to prove that such harm has occurred, or is likely to occur. *See* footnote 38, *infra*.

future. Complaint Counsel replies to this argument that: Section 5(n) does not require proof of actual, completed harms; proof of likely harm is sufficient under Section 5(n); consumers do not necessarily know or investigate when they have suffered identity theft harm; the evidence demonstrates actual harm in the form of reputational and other harms arising from the exposure of the 1718 File; and the evidence demonstrates increased risk and/or significant risk of data breach and resulting injury.

3. Actual or Likely Harm

The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged failure to employ "reasonable" data security for its computer networks, including in connection with the Security Incidents alleged in the Complaint. Complaint Counsel presented no evidence of any consumer that has suffered NAF, ECF, ENCF, medical identity theft, reputational injury, embarrassment, or any of the other injuries Complaint Counsel describes. Complaint Counsel's response -- that consumers may not discover that they have been victims of identity theft, or even investigate whether they have been so harmed, even if consumers receive written notification of a possible breach, as LabMD provided in connection with the exposure of the Sacramento Documents (F. 212) -- does not explain why Complaint Counsel's investigation would not have identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security.

Complaint Counsel's response to the absence of evidence of actual harm in this case, that it is not legally necessary under Section 5(n) to prove that actual harm has resulted from alleged unfair conduct, because "likely" harm is sufficient, *see, e.g.*, CCRFF 295, 414, 455; CCRB at 131-132; CCCL ¶ 25, fails to acknowledge the difference between the burden of production and the burden of persuasion. The express language of Section 5(n) plainly allows liability for unfair conduct to be based on conduct that has either already caused harm, or which is "likely" to do so. *See Wyndham*, 2015 U.S. App. LEXIS 14839, at **21. However, as shown *infra*, the absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years, undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless "likely" to occur. This is

particularly true here, where the claim is predicated on expert opinion that essentially only theorizes how consumer harm could occur. Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.

In light of the inherently speculative nature of predicting "likely" harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted "likely" harm alone. For example, in *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988), the appellate court upheld the Commission's finding of substantial injury, based on undisputed evidence that Orkin's failure to honor consumers' contracts generated, during a four-year period, more than $7 million in revenues from renewal fees paid by consumers to which Orkin was not entitled. In *FTC v. Accusearch, Inc.*, 2007 U.S. Dist. LEXIS 74905 (Sept. 28, 2007), *aff'd*, 570 F.3d 1187 (10th Cir. 2009), on the issue of substantial injury, the court stated: "The range of injuries experienced by the consumers whose phone records were sold fits squarely within the categories of harm contemplated by the FTC's policy," including "documented economic harm" in the form of "actual costs associated with changing telephone carriers and addressing necessary upgrades to the security of the accounts." *Id.* at *23-24.

The substantial consumer injury supporting unfair conduct liability in *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1154 (9th Cir. 2010), was the issuance of fraudulent checks totaling over $4 million, caused by the defendant's faulty "Qchex" system. And, in *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012), the defendant's website marketing of its online auction product caused thousands of consumers to incur unauthorized monthly charges ranging from $29.95 to $59.95, with an approximate total of $18.2 million in consumer losses. *See also FTC v. Windward Mktg., Ltd.*, 1997 U.S. Dist. LEXIS 17114 at *2, *31-32 (N.D. Ga. Sept. 30, 1997) (unauthorized demand drafts paid against consumers' bank accounts as a result of fraudulent telemarketing scheme); *Int'l Harvester*, 1984 FTC LEXIS 2, at *255 (death and serious injury resulting from failure to disclose known defects in respondent's tractors). Finally, in *Wyndham*, 2015 U.S. App. LEXIS 14839, which is the only court case that has upheld the

FTC's authority to bring an unfair conduct claim based upon alleged unreasonable data security, the court, in denying the defendant's motion to dismiss, noted, *inter alia*, that "[o]n three occasions in 2008 and 2009 hackers successfully accessed Wyndham['s] computer systems . . . [and] stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges." *Id.* at **3.

Section 5(n) does not define the meaning of "likely" injury. Where a statute does not define a term, it is construed in accordance with its ordinary meaning. *FDIC v. Meyer*, 510 U.S. 471, 476 (1994) (using Black's Law Dictionary to define the meaning of statutory term, "cognizable"). The Merriam-Webster dictionary states that "likely" is "used to indicate the chance that something will happen," and is primarily defined as "having a high probability of occurring or being true." *Merriam-Webster.com.*, *at* http://www.merriam-webster.com/dictionary/likely). In *Southwest Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1986), the court interpreted the Commission's deception standard, which required proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ." Based on the foregoing, "likely" does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur.

Complaint Counsel argues that the requirement of proving that injury is "likely" can be met by evidence of a "significant risk" of injury, citing a footnote in the Policy Statement in which the Commission stated: "An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, *or if it raises a significant risk of concrete harm*." 1984 FTC LEXIS 2, at *307 n.12 (emphasis added); *see also LabMD*, 2014 FTC LEXIS 2, at *54. However, although Congress refers to the Policy Statement in explaining the meaning of Section 5(n), the Senate Report states in part: "Consumer injury may be 'substantial' under this section if a relatively small harm is inflicted on a large number of consumers *or if a greater harm is inflicted on a relatively small number of consumers*." S. REP. 103-130, 1993 WL 322671, at *13 (emphasis added). The omission of the Commission's "significant risk" language in explaining "substantial injury" indicates that Congress considered but rejected this standard. Congress instead enacted the requirement that, to be declared "unfair," there must be proof that actual harm has occurred, or in the absence of proof of actual, completed harm, proof that the

challenged conduct is "likely" to cause harm in the future. Moreover, although some courts have cited the "significant risk" language from the Policy Statement, *see, e.g.*, *Neovi*, 604 F.3d at 1157, the parties have not cited, and research does not reveal, any case in which unfair conduct liability has been imposed without proof of actual, completed harm, based instead upon a finding of "significant risk" of harm.[26]

Based on the foregoing, to the extent "significant risk," or "increased risk," of injury implies a lower standard of proof than "likely" injury, such a standard would conflict with the express language of Section 5(n). It is unnecessary to resolve any apparent conflict, however, because, as more fully explained below, even under Complaint Counsel's asserted "significant risk" standard for proving likely harm, Complaint Counsel has failed to prove that Respondent's alleged unreasonable data security is "likely" to cause substantial consumer injury.

Section 5(n) is a three-part test, and all three parts must be proven before an act or practice can be declared "unfair." 15 U.S.C. § 45(n). *See Orkin Exterminating Co.*, 849 F.2d at 1364 ("[T]o justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.") (*quoting* Policy Statement at 36); *see also Windward Mktg.*, 1997 U.S. Dist. LEXIS 17114, at *30. Accordingly, Complaint Counsel's failure to meet its burden of proving the first prong of the three part test – that Respondent's conduct caused, or is likely to cause, substantial consumer injury – is fatal to its case, and any factual determinations regarding the additional two prongs of the unfair conduct test – that substantial consumer injury is not

[26] In *American Financial Services v. FTC*, 767 F.2d 957 (D.C. Cir. 1985), the Court of Appeals for the District of Columbia Circuit upheld a credit practices rule that prohibited wage assignments and household good security interests, finding substantial evidence that these practices were unfair. Regarding the evidence of substantial injury in the rulemaking record, the court stated: "The harms to consumers resulting from the use of HHG security interests and wage assignments identified by the Commission on the basis of the rulemaking record are neither trivial or speculative nor based merely on notions of subjective distress or offenses to taste [and therefore they] result in *or* create a significant risk of substantial economic and monetary harm to the consumer as well as potential deprivations of their legal rights." 767 F.2d at 975 (emphasis added). *American Financial Services* is not precedent that liability can be based on a "significant risk of harm" alone, since the rulemaking record in that case contained substantial evidence that the prohibited provisions had indeed caused financial and other harm to consumers. 767 F.2d at 973-75. It should also be noted that *American Financial Services* involved review of a rulemaking, not an adjudication of individual liability, and was decided before the 1994 enactment of Section 5(n). As noted above, the legislative history of Section 5(n) indicates that Congress rejected "significant risk" as a basis for finding substantial consumer injury.

reasonably avoidable by consumers, and is not outweighed by benefits to consumers or competition – would be superfluous and, accordingly, need not, and will not, be made.

4. Complaint Counsel's Proffered Consumer Injury Experts

As noted above, Complaint Counsel's contention that Respondent's alleged unreasonable data security is likely to cause harm is predicated upon expert opinion from two proffered experts, Mr. Rick Kam and Mr. James Van Dyke.

Mr. Kam is president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration, and is a Certified Information Privacy Professional. F. 9. According to Mr. Kam, his expertise includes "identifying and remediating the consequences of identity theft and medical identity theft" and "helping organizations develop policies and solutions" to safeguard sensitive personal information. F. 10. Mr. Kam was asked "to assess the risk of injury to consumers caused by the unauthorized disclosure" of their personal information. F. 11. For the purposes of this analysis, Mr. Kam assumed that LabMD failed to provide reasonable security for consumer information on its computer networks. F. 244. In summary, Mr. Kam opined that LabMD's alleged unreasonable data security "is likely to cause substantial injury to consumers and puts them at significant risk of identity crimes." CX0742 (Kam Expert Report at 9). Mr. Kam's more detailed opinions are addressed *infra* in the context of the particular harms alleged in this case.

Mr. Van Dyke is the founder and president of Javelin Strategy & Research ("Javelin"), a research company whose activities include publishing results from an annual identity fraud survey and an associated report. F. 12. According to Mr. Van Dyke, he is experienced in how sensitive information is used and has expertise in identity theft. F. 14. Mr. Van Dyke was asked to "assess the risk of injury to consumers" whose personally identifiable information "has been disclosed by [LabMD] without authorization." F. 15. He was also asked to assess the risk of injury to those consumers whose information "was not adequately protected from unauthorized disclosure." F. 15. Mr. Van Dyke assumed, as did Mr. Kam, that LabMD failed to provide reasonable security for personal information maintained on its computer networks. F. 257. In general, Mr. Van Dyke opined that consumers whose information was disclosed in the 1718 File and the Sacramento Documents are significantly more likely to become victims of identity theft

and its various subtypes. CX0741 (Van Dyke Expert Report at 3, 6). Mr. Van Dyke also prepared what he called "projections" of the number of such identity theft victims in this case and the financial losses that will result, were identity theft to occur. *Id*. at 6-14. Mr. Van Dyke further opined that LabMD's alleged unreasonable data security "risked exposing" all consumers whose personal information is maintained by LabMD to "a likelihood" of identity theft harm, even if such personal information has not yet been disclosed. *Id.* at 13. The specifics of Mr. Van Dyke's opinions are addressed in relation to the specific harms asserted by Complaint Counsel, *infra*.

5. The 1718 File Incident

a. Summary of facts

The "1718 File" is a LabMD insurance aging report, containing 1,718 pages, dated June 2007, with the filename "insuranceaging_6.05.071.pdf" and is the document identified as the "[peer-to-peer] insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint. F. 1, 73, 78. On or about February 25, 2008, Mr. Richard Wallace, a forensic analyst then employed by a breach detection and remediation services company known as Tiversa Holding Company ("Tiversa"), was performing searches on a peer-to-peer network when he discovered and downloaded the 1718 File. F. 100, 102-104, 121. The 1718 File was downloaded from an IP address in Atlanta, Georgia, which belonged to LabMD. F. 121. These events, further addressed below, are referred to herein as the "1718 File Incident." F. 78.

By way of background, peer-to-peer file-sharing applications enable one computer user to make a request to search for all files that have been made available for sharing by another (or "host") computer that is also using the same file-sharing application. F. 63. A file that is being "shared" or "made available for sharing," on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. F. 66. Typically, users will search using terms related to the particular file they hope to find and receive a list of files that are possible matches. F. 65. The user then chooses a file he or she wants to download from the list, which is then downloaded from the peers who possess that file. F. 65. The contents of a file are not exposed until the file is downloaded. F. 68.

Peer-to-peer networks are often used to share music, videos, pictures, and other materials. F. 64. In 2008, LimeWire was a peer-to-peer file-sharing application, and one of a number of applications that used a protocol called Gnutella. F. 69. Gnutella is a program that connects computers together in a direct peer-to-peer fashion to facilitate file sharing through searching and downloading. F. 70.

In May 2008, Tiversa contacted LabMD and told LabMD that the 1718 File was available through LimeWire. F. 88. LabMD investigated and determined that LimeWire was installed on a computer belonging to LabMD's billing manager (the "Billing Computer") and that the 1718 File was among the files made available for sharing. F. 89-91. After searching all of LabMD's computers, it was determined that no other LabMD computers had file-sharing applications installed. F. 90, 93-94. LabMD removed LimeWire from the Billing Computer in May 2008. F. 92. In addition, Mr. John Boyle, LabMD's vice president of operations and general manager from November 1, 2006 until the end of August 2013, assigned LabMD Information Technology ("IT") Specialist Allison Simmons, and later, IT Manager Jeffrey Martin, to search peer-to-peer networks to look for the 1718 File. F. 95. Specifically, in May 2008, Ms. Simmons searched peer-to-peer networks from her home computer to look for the 1718 File. F. 96. She searched multiple times for at least a month thereafter for the file name insuranceaging_6.05.071.pdf, partial file names, and anything with the name LabMD associated with it. F. 96. In 2013, Mr. Martin searched peer-to-peer networks for the 1718 File multiple times over the course of a few months, using the file name, as well as the terms "LabMD," "patient," and "aging." F. 97. The searches performed by Ms. Simmons and Mr. Martin did not locate the 1718 File on any peer-to-peer network. F. 98.

In addition, in 2009, Mr. Wallace, of Tiversa, searched Tiversa's internal database of peer-to-peer sharing downloads (Tiversa's "Data Store") to determine if Tiversa's automatic searching system, which uses a series of algorithms to search all peer-to-peer networks, had downloaded the 1718 File. F. 100, 147. Mr. Wallace determined that the 1718 File had not been downloaded to the Data Store. F. 147. To Mr. Wallace's knowledge, the 1718 File never spread beyond the original disclosing source, LabMD. F. 154.

In 2008, Tiversa was a "research partner" of Professor Eric Johnson, then of Dartmouth College, in connection with an article that Professor Johnson was writing. F. 169, 170. Tiversa's role in the research was to conduct searches for Professor Johnson and to forward files to him for further analysis. F. 172. All the files examined in Professor Johnson's research for his article were provided to him by Tiversa. F. 172. Professor Johnson referred to the 1718 File in his article, published in February 2009, titled "Data Hemorrhages in the Health-Care Sector." F. 169, 171. Tiversa had provided the 1718 File to Professor Johnson. F. 178. However, the evidence fails to prove that the 1718 File was discovered as a product of Professor Johnson's search protocol, notwithstanding any contrary representation in his article. F. 173-175, 178-179. Professor Johnson did not share the sensitive information in the 1718 File with anyone. F. 181.

In 2009, Tiversa, who had been communicating with the FTC regarding peer-to-peer file-sharing matters (F. 133-134), identified LabMD to the FTC as one of the entities that Tiversa discovered had shared personal information of consumers on peer-to-peer networks. F. 139-142. Tiversa also provided the 1718 File to the FTC.[27] F. 138.

b. Overview of analysis

Complaint Counsel argues that the exposure of the 1718 File on the Gnutella network constitutes evidence that Respondent's data security practices are likely to cause substantial harm, and that consumers whose Personal Information was exposed in the 1718 File are at "significantly higher risk than the general public of becoming a victim of identity theft and medical identity theft, or of experiencing other privacy harms[. Therefore,] the failure to secure the 1718 File is likely to cause them substantial injury." CCB 69. Respondent argues that other than Tiversa, Professor Johnson, and the FTC, no one outside of LabMD downloaded or viewed

[27] Tiversa did not want the FTC to issue a formal information request, such as a Civil Investigative Demand ("CID"), directly to Tiversa because Tiversa had been in talks regarding a possible acquisition and Tiversa's chief executive officer, Mr. Boback, did not want Tiversa to be "in the middle of a civil investigative demand." F. 135. Instead, Mr. Boback wanted the CID to be issued to a third party to "separate" the CID from Tiversa, "to try to create some distance" from Tiversa. F. 135. Accordingly, Tiversa created an entity called "The Privacy Institute," so Tiversa could avoid providing information to the FTC under Tiversa's name. F. 136. The Privacy Institute was created only for the purpose of receiving the CID from the FTC. F. 136. Upon Tiversa's request, the FTC issued the CID for Tiversa's information and documents to the Privacy Institute. F. 137-138. Whether or not this entire process met the requirements of all applicable law, rules, and regulations has not been determined in the instant case.

the contents of the 1718 File. Respondent further argues that there is no evidence that any consumer has suffered any harm from the exposure of the 1718 File.

The evidence shows that the 1718 File was available for peer-to-peer sharing through LabMD no earlier than June 2007 (the date of the document) until May 2008, when Respondent removed LimeWire from the Billing Computer. F. 78, 92, 99. Although the 1718 File was available for downloading during this period, the evidence fails to show that the 1718 File was in fact downloaded by anyone other than Tiversa, who obtained the document in February 2008. Tiversa provided the 1718 File to Professor Johnson and to the FTC. F. 138, 142, 178. Evidence in the record provided by Tiversa and its chief executive officer and corporate designee Mr. Robert Boback, claiming that Tiversa found the 1718 File in "multiple locations" on peer-to-peer networks, including at IP addresses belonging to suspected or known identity thieves, is given no weight. As summarized in Section I.B.2., and detailed in Section II.D.3. and 4., *supra*, such evidence, including without limitation, Mr. Boback's 2013 discovery deposition, Mr. Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Wallace. Furthermore, Complaint Counsel no longer argues, as it did in its pre-trial brief, that the 1718 File was in fact downloaded by anyone other than Tiversa. In summary, Complaint Counsel has failed to prove that the 1718 File was acquired, viewed, or otherwise disclosed to anyone other than Tiversa, Professor Johnson, and the FTC. Any other assertion or conclusion regarding the extent of the exposure of the 1718 File is pure, unsupported speculation.

As further discussed below, the evidence fails to demonstrate that the exposure of the 1718 File placed the consumers whose Personal Information was exposed in the 1718 File "at significantly higher risk" of harm, or that such exposure caused, or is likely to cause, identity theft harm, medical identity theft harm, or reputational or "other" harm, as argued by Complaint Counsel.

c. Identity theft harm

i. Mr. Rick Kam

Complaint Counsel's arguments, that consumers whose information was contained in the

1718 File are at "significantly higher risk" of becoming victims of identity theft, and are "likely" to suffer identity theft harm, rely on the opinion of its proffered expert, Mr. Kam. *See* CCB at 69, *citing* CCFF 1667, 1668. Mr. Kam evaluated the risk of identity theft harm resulting from an unauthorized disclosure of personal information on the basis of four risk factors, including: (1) the nature of the information exposed; (2) "to whom the disclosure was made [in order] to determine whether the person possessing the information presents a low risk of misuse, or a higher risk of misuse, such as an identity thief"; (3) whether the information was "actually acquired or viewed"; and (4) whether "the data is still available for others to misuse." F. 238-239. Mr. Kam then applied the foregoing risk factors to conclude that the exposure of the 1718 File poses a significant risk of identity theft harm. CX0742 (Kam Expert Report at 18-19).

Although Complaint Counsel announced it would not rely on expert opinion based on the testimony of Mr. Boback or on CX0019, *see* Section I.B.2., *supra*, Mr. Kam's opinion, upon which Complaint Counsel does rely, is expressly based on evidence provided by Mr. Boback that Tiversa had found the 1718 File at various IP addresses between 2008 and 2011; that one of the IP addresses belonged to a suspected identity thief; and that Tiversa found the 1718 File to be still available on peer-to-peer networks in 2013. F. 240-241.[28] As discussed above, this evidence is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Wallace. For this reason, Mr. Kam's opinions that the exposure of the 1718 File is likely to cause, or presents a "significant risk" of, identity theft harm is entitled to, and is given, no weight.

Indeed, applying Mr. Kam's four risk factors, above, to the facts of this case, it is at least as likely, if not more likely, that the exposure of the 1718 File presents a low risk of identity theft harm. In the instant case, the evidence fails to show that the 1718 File was disclosed to and viewed by anyone other than Tiversa, Professor Johnson, and the FTC, and there is no contention, or evidence, that the foregoing persons or entities present a threat of harming consumers. This is in stark contrast to cases relied upon by Complaint Counsel where Personal Information was allegedly obtained by computer hackers and used to commit credit card fraud.

[28] *See also* Kam, Tr. 519 (explaining that he relied upon a report published by the SANS Institute, the SANS Health Care Cyberthreat Report, published in 2014, based upon Mr. Boback's discredited testimony about the discovery of the 1718 File on a peer-to-peer network in 2013).

See Wyndham, 2015 U.S. App. LEXIS 14839, at **3 (court stating that hackers accessed Wyndham's computer systems on three occasions and stole personal and financial information leading to over $10.6 million dollars in fraudulent charges); *Remijas v. Neiman Marcus Group, LLC*, 2015 U.S. App. LEXIS 12487 at **2-3, **8-13 (7th Cir. July 20, 2015) (court stating that hackers accessed Neiman Marcus' computer systems and stole financial information leading to fraudulent use of 9,200 consumers' credit cards).

Significantly, the court in *Neiman Marcus*, in concluding that the plaintiffs had demonstrated sufficient injury to obtain Article III standing, remarked: "[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Neiman Marcus*, 2015 U.S. App. LEXIS 12487 at **12. Here, in contrast, the evidence fails to show any computer hack for purpose of committing identity fraud. Rather, the evidence shows that the 1718 File was obtained by Tiversa from a peer-to-peer network, F. 121-122, and that Tiversa's purpose in obtaining this and other files available from peer-to-peer networks was to then induce companies with an interest in protecting such information to purchase Tiversa's monitoring or remediation services. F. 100, 108-118. Unlike in *Neiman Marcus*, it cannot be presumed that the purpose of Tiversa's act of downloading the 1718 File from a peer-to-peer network was to make fraudulent credit card charges, assume identities, or otherwise harm the consumers whose information is contained in the 1718 File.

In addition, the evidence shows that the 1718 File was no longer available for sharing by LabMD as of May 2008 (F. 99), and the evidence fails to show that the 1718 File remained available on peer-to-peer networks after May 2008. *See* F. 95-98, 153-154. For this reason as well, the evidence fails to prove that the exposure of the 1718 File presents a significant risk of identity theft harm or is likely to cause identity theft harm.

ii. Mr. James Van Dyke

Complaint Counsel's assertion that consumers whose Personal Information was exposed in the 1718 File are at significantly higher risk than the general public of suffering identity theft harm is also based upon the opinions of Mr. Van Dyke, which Mr. Van Dyke derived from the

Javelin 2013 Identity Fraud Survey ("2013 Javelin Survey") and the Javelin 2014 Identity Fraud Report ("2014 Javelin Report"). CCB at 69, citing CCFF 1506-1512; F. 252. As noted above, Mr. Van Dyke, is the founder and president of Javelin. F. 12.

Specifically, Complaint Counsel relies on a statistic reported in the 2013 Javelin Survey that 30.5% of survey respondents who reported being notified within the 12 months preceding the survey that their "personal or financial information ha[d] been lost, stolen, or compromised in a data breach (*i.e.*, data breach victims)," also reported experiencing identity theft within the 12 months preceding the survey ("identity theft rate"). CX0741 (Van Dyke Expert Report at 6-8 and Attachment 1). The 2013 Javelin Survey further stated that 2.7% of those survey respondents who reported they had *not* been notified during the 12 months preceding the survey that they were data breach victims also reported suffering identity theft harm during that same 12-month period. CX0741 (Van Dyke Expert Report at 6-8). Accordingly, Complaint Counsel argues, consumers whose information was exposed in the 1718 File are at a "significantly higher risk" or have an "increased risk" of becoming identity theft victims, and are therefore likely to suffer identity theft harm.[29]

Complaint Counsel also relies on Mr. Van Dyke's projections of the number of 1718 File consumers that will become identity theft victims, and the monetary losses that these consumers will incur as a result. According to Mr. Van Dyke, based on the 2013 Javelin Survey: (1) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their Social Security number ("SSN") was disclosed in a data breach also reported experiencing new account fraud within the preceding 12 months, at an average consumer loss of $449; (2) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing non-card fraud within the preceding 12 months, at an average consumer loss of $207; and (3) 13.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing

[29] Mr. Van Dyke also opined that "[t]he circumstances of the unauthorized exposure of the" 1718 File "only stand to make identity fraud more likely" than the 30% identity theft rate found in the 2013 Javelin Survey, based on Mr. Boback's discredited testimony that the 1718 File "was found at four IP addresses, on each of which Tiversa found unrelated consumer identity information." CX0741 (Van Dyke Expert Report at 8). Complaint Counsel does not rely on this particular opinion in its brief or proposed findings of fact.

existing card fraud within the preceding 12 months, at an average consumer loss of $106. CX0741 (Van Dyke Expert Report at 8-12). Mr. Van Dyke applied these percentages and figures to the number of consumers listed in the 1718 File to calculate the number of expected identity theft victims and the expected financial impact. *Id*. However, Mr. Van Dyke did not conduct a survey of the consumers listed on the 1718 File. F. 255.

For several reasons, the 2013 Javelin Survey, the 2014 Javelin Report, and Mr. Van Dyke's opinions based thereon, are not persuasive in proving that those consumers whose Personal Information was exposed in the 1718 File are likely to suffer identity theft harm. First, and perhaps most important, Complaint Counsel's suggested inference, based on the 2013 Javelin Survey, that 30% of the consumers whose data was contained in the 1718 File have suffered, or will suffer, identity theft harm, is unpersuasive, in light of the absence of any evidence that any such consumer, in fact, has been so harmed, despite the passage of more than seven years since exposure of the 1718 File. If it were true that 30% of the consumers affected by the 1718 File exposure are likely to suffer identity theft harm, logically, it would be expected that the government, in the many years of investigation and litigation of this matter, would have discovered and identified at least one such consumer who has experienced identity theft harm. The same logic renders unpersuasive Mr. Van Dyke's predictions of the number of consumers that will suffer NAF, ECF, or ENCF and resulting monetary losses.

As noted above, Complaint Counsel's assertion, based on expert opinion, that it may take "months or years" for a consumer to discover they have been victimized by identity theft (*see* CCFF 1578-1580), does not explain why the government, over the past seven years, in the course of investigating and litigating this case, would not have located and identified any such victims. *See* Section III.D.2., 3. In summary, in the instant case, the absence of evidence that identity theft harm has occurred in the seven years since the exposure of the 1718 File undermines the persuasive value of expert opinion that such harm is, nonetheless, "likely" to occur. *See In re McWane, Inc.*, 2013 FTC LEXIS 76, at *730-31 (May 8, 2013) (finding that the absence of evidence that prices rose after alleged agreement to raise prices undermined assertion that such agreement existed). Fairness dictates that reality must trump speculation based on mere opinion.

Second, results from the 2013 Javelin Survey are not probative as a temporal matter. As discussed above, the 1718 File was made available for sharing no earlier than June 2007; LabMD discontinued its sharing of the document in May 2008; and the evidence fails to show that the 1718 File was available on peer-to-peer networks after May 2008. The 2013 Javelin Survey measured the effect of data breaches occurring five years later, in 2013, and Complaint Counsel points to no evidence from which it could be concluded that the incidence of identity theft for exposures in 2013 is predictive of identity theft harm for an exposure five years earlier, in 2008. Indeed, rather than select and use data from 2008, the most relevant point in time, Mr. Van Dyke selected the 2013 Javelin Survey and 2014 Javelin Report for the bases of his calculations specifically because, in 2013, Mr. Boback testified that Tiversa had located the 1718 File on peer-to-peer networks in four locations, which testimony has been thoroughly discredited. F. 253. Moreover, according to the yearly Javelin Identity Fraud surveys for 2010 through 2013, as set forth in Mr. Van Dyke's report, the identity fraud rate for data breach victims in 2013 was significantly higher than the identity fraud rate for data breach victims in 2010, a point closer in time to the exposure of the 1718 File. CX0741 (Van Dyke Expert Report at 8, Figure 1 (depicting 11.8% rate in 2010, 18.9% rate in 2011, 22.5% in 2012, and 30.5% in 2013)).

Third, it is not apparent that the data breach victims surveyed by the 2013 Javelin Survey are similarly situated to the consumers whose Personal Information was exposed in the 1718 File, such that any identity theft rate derived from the 2013 Javelin Survey can be extrapolated to predict identity theft harm for the 1718 File consumers. As noted above, the limited time duration that the 1718 File was available for downloading, and the limited extent of actual exposure of the 1718 File, including the fact that the 1718 File was downloaded by Tiversa for business purposes, and not for identity theft purposes, are factors that militate against the risk of identity theft harm in this case. The evidence fails to show the types of data breaches reported in the 2013 Javelin Survey are comparable to the type of data exposure that occurred in the 1718 File Incident.

For all the foregoing reasons, the evidence fails to show that the exposure of the 1718 File has caused, or is likely to cause, identity theft harm.

d. Medical identity theft harm

Relying on expert opinion, Complaint Counsel asserts that the exposure of the 1718 File is likely to result in medical identity theft harm. *See* CCB at 70-71. Specifically, Mr. Van Dyke opined that "medical identity fraud remains a threat to consumers," citing survey responses as to the frequency of medical identity theft. He further opined that health insurance policy information and SSNs, which are found in the 1718 File, "can be utilized" by criminals to commit medical identity frauds, such as procuring procedures, services, and products. CX0741 (Van Dyke Expert Report at 13-14). Mr. Van Dyke also opined that such frauds, when they occur, "can burden affected consumers with financial costs related to unpaid medical bills from unauthorized procedures, products, or services, as well as direct physical harm in those cases where a change is made to a consumer's medical records that could result in improper or unnecessary treatments." *Id.* The foregoing is not an opinion that medical identity theft is likely to result from the exposure of the 1718 File, but is little more than a statement of Mr. Van Dyke's belief that identity theft criminals "could" use information in the 1718 File, if they obtained it, and his opinion of the financial and other harms that "could" result, if medical identity theft were to occur. However, the evidence fails to show that any identity theft criminals have obtained the 1718 File, and therefore the projection of resulting harms from medical identity theft is pure theory and speculation.

Complaint Counsel also relies on predictions by Mr. Kam that the 1718 File consumers are subject to "health and safety" risks resulting from medical identity theft, such as misdiagnosis or mistreatment of illness. CX0742 (Kam Expert Report at 20). Mr. Kam explained that if an identity thief's health information "merges" with that of the identity theft victim, inaccuracies in medical records could result and cause mistreatment or misdiagnoses. Kam, Tr. 426-430. Mr. Kam further predicted, derived from an "estimated base rate" for medical identity theft of 0.0082, that at least 76 of the 9,300 consumers identified in the 1718 File will become victims of medical identity theft, and that 36% of these individuals will each suffer out-of-pocket costs for fraudulently procured medical services among other expenses in the amount of $18,660. CX0742 (Kam Expert Report at 19-20).[30] Mr. Kam based these

[30] Mr. Kam opined that these losses from medical identity theft include payments required as a result of a "lapse" of health insurance. (Kam, Tr. 422). However, Mr. Kam failed to explain this assertion.

opinions on statistics as to the frequency and impact of medical identity theft reported by the 2013 Survey on Medical Identity Theft by the Ponemon Institute ("2013 Ponemon Survey"). F. 246. Mr. Kam's opinions are unpersuasive to demonstrate that the exposure of the 1718 File is likely to cause medical identity theft harm, as explained below.

As stated previously, there is no evidence that any consumer has suffered any of Mr. Kam's predicted harms as a result of the exposure of the 1718 File, notwithstanding the passage of more than seven years since the exposure of the 1718 File in 2008.[31] Furthermore, the 2013 Ponemon Survey lacks significant probative value, given that it measured the rate and impact of medical identity theft for 2013, five years after the 2008 disclosure of the 1718 File. *See* F. 246. Moreover, numerous facts detract from the reliability of the 2013 Ponemon Survey. The response rate to the 2013 Ponemon Survey was only 1.8%, which Mr. Kam agreed creates a non-response bias, *i.e.*, a failure to take into account that those who were surveyed, but did not respond, might have a different answer to the question. F. 247. In addition, the 2013 Ponemon Survey had a sampling frame bias[32] and compensated respondents for completing the survey within a set time period. F. 248-249. Also significant is that, to the extent the 2013 Ponemon Survey is reliable, the accompanying report notes that medical identity theft rarely occurs from data breaches or the acts of an identity thief. F. 250. Rather, the 2013 Ponemon Survey reports that medical identity theft is far more likely to result from a consumer's knowingly sharing personal identification or medical credentials or the unauthorized use of such information by a family member. F. 250. Mr. Kam agreed that medical identity theft rarely occurs from data breaches or the acts of an identity thief and acknowledged that most occurrences of medical identity theft result from someone knowingly sharing their personal information or medical credentials and from instances where one family member took another family member's personal information or medical credentials without consent. F. 251.

[31] Although Mr. Kam did not expressly rely on the discredited and unreliable testimony from Mr. Boback as to the "spread" of the 1718 File for his opinions on the likelihood of medical identity theft, this evidence was clearly considered by Mr. Kam (CX0742 (Kam Expert Report at 6)) and it cannot be assumed that Mr. Kam's opinions were not influenced by his review of Mr. Boback's testimony.

[32] The 2013 Ponemon Survey's sampling frame contained individuals who were prescreened from a larger sample on the basis of their identity theft or identity fraud experience. The 2013 Ponemon Survey acknowledged, and Mr. Kam agreed, that this resulted in a sampling frame bias. F. 248.

For all the foregoing reasons, the evidence fails to support the conclusion that medical identity theft harm is likely to result from the exposure of the 1718 File that occurred in this case.

e. Reputational and other harms

Finally, relying on expert opinion from Mr. Kam, Complaint Counsel argues that the exposure of the 1718 File alone, without any resulting identity theft, is likely to cause "reputational and other harms" to those consumers. Specifically, Complaint Counsel asserts that the 1718 File disclosed some current procedural terminology ("CPT") codes that indicate testing for "sensitive conditions," such as sexually transmitted diseases, including HIV, prostate cancer and testosterone levels, and that disclosure of such testing causes harm in the form of stigma or embarrassment. *See* CCB at 71.

Mr. Kam opined that there is a "significant risk" of reputational harm for those consumers whose CPT codes indicate tests for prostate cancer, herpes, hepatitis, HIV, and testosterone levels. Kam, Tr. 447-448; CX0742 (Kam Expert Report at 9). Further, he opined that disclosure of the mere fact that such a test was performed, even without disclosure of any associated condition or diagnosis, "could cause" consumers to feel embarrassed, upset, or stigmatized. Kam, Tr. 448; CX0742 (Kam Expert Report at 16, 21).[33] However, as Mr. Kam acknowledged, disclosure of a CPT code, by itself, does not disclose what test was performed. F. 83. In fact, Mr. Kam testified that he had to rely on a Google search to determine what the CPT codes stood for. F. 83. Moreover, given the subjective nature of feelings of stigma, upset, or embarrassment, and the fact that Complaint Counsel did not identify a single person affected by the 1718 File disclosure who experienced these feelings as a result of the 1718 File disclosure, expert opinion that these feelings "can" occur carries little or no weight. *Compare Accusearch*, 2007 U.S. Dist. LEXIS 74905, at *23-24 (noting undisputed fact that some consumers whose phone records were sold to stalkers and abusers had suffered actual and severe emotional harm).

[33] Mr. Kam also opined that exposure of CPT codes could lead to negative changes to life, health, and disability insurance. CX0742 (Kam Expert Report at 21). However, Mr. Kam failed to persuasively explain how disclosure of the mere fact that testing was performed, without further information, could result in negative changes to insurance.

In addition, subjective feelings such as embarrassment, upset, or stigma, standing alone, do not constitute "substantial injury" within the meaning of Section 5(n). According to the legislative history of Section 5(n), "[e]motional impact and more subjective types of harm alone are not intended to make an injury unfair." S. REP. 103-130, 1993 WL 322671, at *13; *see also* 1982 Policy Letter, *reprinted in* H.R. Rep. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) ("As a general proposition, substantial injury involves economic or monetary harm and does not cover subjective examples of harm such as emotional distress . . ."). While the Commission has stated that "[i]n an extreme case, . . . where tangible injury could be clearly demonstrated, emotional effects might possibly be considered as the basis for a finding of unfairness," Policy Statement, 1984 FTC LEXIS 2, at *308 n.16, in the instant case, there is no demonstrated tangible injury to consumers from the exposure of the 1718 File. *Compare Accusearch*, 2007 U.S. Dist. LEXIS 74905, at *22-24 (finding conduct caused economic harm and health and safety risks in addition to emotional harm).

Accordingly, the evidence fails to prove that consumers are likely to suffer the asserted "reputational and other harms" as a result of the exposure of the 1718 File. Even if the evidence demonstrated such harms, because the evidence fails to show any tangible injury from the exposure of the 1718 File, the subjective "reputational and other harms" alleged by Complaint Counsel do not constitute sufficient "substantial injury" under Section 5(n).

f. Conclusion

For all the foregoing reasons, the evidence fails to prove that consumers whose information was contained in the 1718 File have suffered, or are likely to suffer, substantial injury as a result of the exposure of the 1718 File. Therefore, the exposure of the 1718 File does not support Complaint Counsel's assertion that Respondent's data security practices are likely to cause substantial consumer harm.[34]

[34] Complaint Counsel also argues that consumer harm is likely from the 1718 File Incident because the 1718 File was made available for sharing on the Gnutella network where any Gnutella user "could" access it. CCB at 69. Evidence that anyone "could" have accessed the 1718 File during the limited period that the 1718 File was made available for sharing carries little probative weight, especially since the evidence fails to show that anyone other than Tiversa, Professor Johnson, and the FTC actually viewed the 1718 File; or that any consumer listed in the 1718 File, in the seven years since the exposure of the 1718 File, has actually suffered any harm as a result of the availability of the 1718 File.

6. The Sacramento Incident

a. Summary of facts

On October 5, 2012, officers of the Sacramento California Police Department (the "SPD") conducted a search of a house in Sacramento, California in connection with an investigation into possible utility bill fraud. F. 189-192. In that house, the SPD discovered what was believed to be evidence of utility billing theft and gas utility bill identity fraud, as well as narcotics paraphernalia and narcotics. F. 191. The SPD also discovered in that house approximately 40 LabMD day sheets, 9 copied checks payable to LabMD, and 1 money order payable to LabMD. F. 182. The day sheets found in Sacramento (the "Day Sheets"), together with the money order found in Sacramento, and the check copies found in Sacramento (the "Check Copies") are collectively referred to herein as the "Sacramento Documents," and this event is referred to herein as the "Sacramento Incident." F. 182.

The Personal Information contained in the Day Sheets consisted of names and what appear to be Social Security numbers for approximately 600 consumers. F. 183. All but two of the Day Sheets are dated between 2007 and 2008. F. 184. The remaining two Day Sheets are from March 2009. F. 184. The Check Copies contained names and bank account numbers for nine consumers, and addresses for all but one of the nine consumers. F. 185. The Check Copies are dated from May 2007 to March 2009. F. 186. The money order, dated August 2008, contained no Personal Information. F. 185, 187.

Two individuals found at the Sacramento house were arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. F. 193. The Sacramento Documents were seized by the SPD and booked into evidence by the SPD. F. 195. The arrested individuals subsequently pled *nolo contendere*[35] to identity theft. F. 194.

[35] "*Nolo Contendere*" is "Latin for 'no contest.' In a criminal proceeding, a defendant may enter a plea of *nolo contendere*, in which he does not accept or deny responsibility for the charges but agrees to accept punishment. The plea differs from a guilty plea because it cannot be used against the defendant in another cause of action." Wex Legal Dictionary, published by Legal Information Institute at Cornell Law School. *See* https://law.cornell.edu/wex/nolo_contendere.

After finding the Sacramento Documents, Detective Karina Jestes of the SPD performed an Internet search and learned that the FTC was investigating LabMD. F. 209. Approximately one week after the October 5, 2012 discovery of the Sacramento Documents, Detective Jestes contacted the FTC regarding the Sacramento Documents. F. 209. In December 2012, the SPD provided the Sacramento Documents to the FTC. F. 210. The SPD made the determination not to return the Sacramento Documents to LabMD based on the FTC's investigation of LabMD. F. 210. On January 30, 2013, the FTC notified LabMD that the FTC had the Sacramento Documents. F. 211. On March 27 or 28, 2013, LabMD sent 682 letters to the consumers named in the Sacramento Documents notifying them of the Sacramento Incident, describing steps such as registering a fraud alert with credit bureaus, offering one year of free credit monitoring services, and inviting consumers to contact LabMD with questions or concerns. F. 212.

b. Summary of arguments

Relying on opinions from Mr. Kam and Mr. Van Dyke, Complaint Counsel argues that the disclosure of Personal Information for approximately 600 consumers in the Sacramento Documents is likely to cause identity theft harm. CCB at 71-72. Complaint Counsel contends that identity theft harm is likely because the types of personal information found in the Sacramento Documents, such as names and Social Security numbers on the Day Sheets, and bank routing and account numbers on the Check Copies, "can be used" by identity thieves to commit identity theft; Social Security numbers "can be used" fraudulently for extended periods of time because they are rarely changed; and there is a "likelihood" the Sacramento Documents "may have" been misused because the documents were found in the possession of individuals who later pleaded no contest to identity theft charges. CCB at 71-72. Complaint Counsel further contends, based on identity theft rates reported by the 2013 Javelin Survey, that "[c]onsumers will incur" approximately $36,000 in monetary losses from "164 cases of" NAF, ENCF, and ECF, and that "consumers will also spend 2,497 hours" resolving the resulting fraud. CCB at 72.

Respondent argues that the Sacramento Documents were found in paper form, and that Complaint Counsel has failed to prove how the documents were taken from LabMD, or how they ended up in California. Moreover, Respondent contends, there is no evidence of any consumer becoming a victim of identity theft because of the disclosure of the Sacramento Documents,

which casts doubt on Complaint Counsel's proffered expert opinions that such harm is "likely." Respondent also challenges the experts' methodology and the evidentiary bases for their opinions.

As explained below, Complaint Counsel has failed to prove that Respondent's alleged failure to reasonably secure data on its computer network caused, or is likely to cause, harm to consumers due to the exposure of the Sacramento Documents. First, Complaint Counsel has failed to prove that the Sacramento Documents were maintained on Respondent's computer network. *See* Complaint ¶ 10 (alleging Respondent failed to provide reasonable "security for personal information on its computer networks"). Second, even if there were a causal connection between Respondent's computer network and the exposure of the Sacramento Documents, the evidence fails to prove that the exposure of these documents has caused, or is likely to cause, any consumer injury.

c. Connection to LabMD's computer network

As part of its billing process, LabMD produced a report that it refers to as a "day sheet" transaction detail to ensure payments were received and posted. F. 198. Day sheets were created electronically through LabMD's billing application, Lytec. F. 199. Once day sheet reports were printed, there was no electronic record of the day sheet in LabMD's system. F. 203. Day sheets were not saved electronically. F. 203. Rather, day sheets were printed almost daily, and stored in paper files at LabMD. F. 203-204, 206. In addition, LabMD made paper copies of patient checks it received, which were retained by the billing department, and originals were shredded after six months. F. 61, 202. While the evidence shows that some LabMD day sheets and check copies may have been scanned and saved to LabMD's computer network as part of an archiving project undertaken by LabMD in or around January 2013 (F. 208), the evidence fails to show that the day sheets and copied checks *that were found in Sacramento* had been scanned and archived, or otherwise saved, onto LabMD's computer network. In fact, the Sacramento Documents were found in October 2012, months before LabMD even began to scan and archive any day sheets or check copies. F. 182, 208. These facts, combined with the fact that the Sacramento Documents were found in physical, and not electronic form (F. 197), weigh against any inference that the

Sacramento Documents were even available from Respondent's computer network, much less exposed as a result of LabMD's alleged unreasonable computer security.[36]

Complaint Counsel asserts that billing employees had "the option" of saving day sheets electronically to a computer, CCFF 156, citing deposition testimony from a former LabMD employee who worked in LabMD's billing department, identified in this Initial Decision as "the Former LabMD Employee." *See* footnote 18. However, although the Former LabMD Employee testified that the software "allowed" a user to save a day sheet or to print it, the Former LabMD employee was clear that she never saved day sheets and did not know of any LabMD employee who had saved a day sheet. F. 207. Complaint Counsel points to no evidence that any employee did electronically save any day sheets, even if it were possible to do so. In addition, although Complaint Counsel points to evidence that the SPD conducted forensic examinations of computers found in the Sacramento house where the Day Sheets and Check Copies were found, *see* CCFF 1447-1452, Complaint Counsel does not assert that these examinations found any connection to LabMD, or to LabMD's computer network.[37] In summary, the evidence upon which Complaint Counsel relies fails to prove that the Sacramento Documents were either available on, or obtained from, LabMD's computer network.

Strangely, Complaint Counsel takes no position as to how the Sacramento Documents came into the possession of the individuals in Sacramento, and further admits that "there is no conclusive explanation of how LabMD Day Sheets were exposed." CCRB at 38; *see also* Transcript of Oral Argument at 54 ("We have not presented evidence of how those documents left the possession of LabMD"); Transcript of Oral Argument at 56 ("We have -- we have made

[36] The Complaint addresses Respondent's computer network security, and does not allege that Respondent's physical security was inadequate, or that inadequate physical security constitutes an "unfair" practice under Section 5. Accordingly, Complaint Counsel's insinuation in its post-trial briefing that Respondent failed to adequately secure paper copies of the Day Sheets and Check Copies (CCRB at 38, CCFF 157-159) is outside the scope of the Complaint and, therefore, will not be considered.

[37] Evidence that a laptop seized from the Sacramento house had LimeWire installed does not prove a connection between the Sacramento Incident and LabMD's computer network. *See* CCFF 1451. The evidence shows that LabMD removed LimeWire in May 2008, and there is no contention that LimeWire or any other peer-to-peer sharing application was present on any LabMD computer after May 2008, including at the time the Sacramento Documents were discovered in October 2012. Nor is there any contention that the Sacramento Documents were at any time made available for sharing via LimeWire or another peer-to-peer application.

no representations regarding how the information left LabMD.”). In related litigation between the parties, in which Respondent sought a preliminary injunction against these administrative proceedings, the district judge stated that “the FTC informed the Court that it was unaware whether the alleged identity thieves arrested in Sacramento” received the Sacramento Documents “as a consequence of LabMD’s data security failures.” *LabMD, Inc. v. FTC*, 2014 U.S. Dist. LEXIS 65090, at *3 n.2 (N.D. Ga. May 12, 2014); *see also LabMD, Inc. v. FTC*, No. 1:14-cv-810, Hr’g Tr. at 77, 80-81 (N.D. Ga. May 9, 2014) (cited in Respondent’s motion for sanctions, filed August 14, 2014) (court exclaiming, “holy cow” in response to FTC’s failure to prove chain of custody with respect to the Day Sheets).

The burden is on Complaint Counsel to prove the allegations of the Complaint that the exposure of the Sacramento Documents was caused by Respondent’s alleged failure to reasonably secure its computer networks. 16 C.F.R. § 3.43(a). *See* Complaint ¶¶ 10, 21, 22. Because the evidence fails to prove that the Day Sheets and Check Copies were taken from LabMD’s computer network, it would require unacceptable and unsupported speculation to conclude that the Sacramento Documents were exposed because of LabMD’s alleged unreasonable computer security. Accordingly, Respondent’s alleged failure to reasonably secure data on its computer network cannot properly be deemed the “cause” of any resulting harm.

Moreover, even if there were a causal connection between Respondent’s alleged unreasonable data security and the exposure of the Sacramento Documents, the evidence fails to prove that the disclosure of the Sacramento Documents has resulted, or is likely to result, in any identity theft harm, as explained below.

d. Identity theft harm[38]

i. Mr. Rick Kam

(a) Opinions

Mr. Kam opined that the consumers whose Personal Information was exposed in the Sacramento Documents are "at risk of harm from identity crimes." CX0742 (Kam Expert Report at 10). Mr. Kam applied his four factor risk assessment, summarized in Section III.D.5.c., *supra*, noting that the Sacramento Documents included names, Social Security numbers, and bank account information which "could be used to commit identity theft" and that "known identity thieves" were found in the possession of the documents, which "increases the possibility that the crime occurred," notwithstanding that Detective Jestes of the SPD "could not confirm that the identity thieves used this data to commit identity fraud." CX0742 (Kam Expert Report at 22). With respect to the mitigation factor of Mr. Kam's four factor risk assessment, Mr. Kam stated that LabMD's written notification to consumers about the Sacramento Incident, offering tools such as credit monitoring, mitigated "some of the risk," but there remains a "strong possibility some of the" affected consumers will still become identity theft victims. CX0742 (Kam Expert Report at 22). Mr. Kam's opinions, summarized above, do not constitute persuasive evidence that identity theft is likely to occur as a result of the exposure of the Sacramento Documents. Mr. Kam's opinions describe little more than the possibility of future harm, or an unquantified, inchoate "risk" of future harm.

Moreover, other evidence weighs against the conclusion that the exposure of the Sacramento Documents has caused, or is likely to cause, harm. In Mr. Kam's experience with data breaches, in each case some individual has come forward to report identity theft harm, which, as Mr. Kam acknowledged, is not the case here. F. 242. Furthermore, there is no

[38] As noted in Section III.D.2.n.25, *supra*, Complaint Counsel's Post-Trial Brief and Proposed Findings of Fact do not address the likelihood of medical identity theft from the exposure of the Sacramento Documents. *See* CCB at 71-72; CCFF § 8.4. Mr. Kam's report does not contain an opinion on the likelihood of medical identity theft from the exposure of the Sacramento Documents. Mr. Van Dyke's expert report contained only a cursory opinion on the likelihood of medical identity theft generally (also referenced in Section III.D.5.d., *supra*) that "health insurance policy information and SSNs can be utilized by criminals to commit medical identity frauds . . ." CX0741 (Van Dyke Expert Report at 13). The Sacramento Documents do not contain health insurance policy information. F. 183, 185. To the extent Complaint Counsel asserts that the exposure of the Sacramento Documents is likely to cause medical identity theft harm, the evidence fails to prove that such harm has occurred, or is likely to occur.

evidence that the individuals found in possession of the Sacramento Documents had used the documents to commit identity theft prior to their arrest, and the likelihood of future misuse is reduced or eliminated by the fact that the Sacramento Documents were seized by the SPD and booked into evidence. F. 195.

In addition, Mr. Kam's opinion of the risk of harm from the exposure of the Sacramento Documents was based in part on the assertion that "approximately 100 SSNs . . . appear to have been used by people with different names," which according to Mr. Kam, "is an indicator that identity thieves may have used this information to commit identity theft." CX0742 (Kam Expert Report at 23). However, this assertion was based on an FTC staff analysis of information obtained from a Thompson Reuters Corporation (Thompson Reuters) database known as CLEAR,[39] which, as detailed below, was excluded for lack of foundation as to the authenticity and reliability of CLEAR's source data. (Tr. 372, *in camera*). For this reason as well, Mr. Kam's opinion regarding likely harm is given little weight.

(b) Exclusion of CX0451

To support Complaint Counsel's claim of identity theft harm resulting from the exposure of the Sacramento Documents, Complaint Counsel proffered a spreadsheet identified as CX0451. According to Complaint Counsel, CX0451 shows that apparent Social Security numbers appearing in connection with persons identified in the Day Sheets have been used by people with different names, which the Complaint alleges "may indicate that the SSNs have been used by identity thieves." *See* Complaint ¶ 21. Respondent objected to the admission of CX0451 on the ground, *inter alia*, of hearsay. Respondent noted that CX0451 is based upon multiple levels of hearsay; the CLEAR database, which forms the basis for CX0451, contains information from various sources that have not been substantiated; and no one had appeared from Thompson Reuters to provide a proper foundation for the reliability of the data contained in the CLEAR database. (Tr. 344, 348-351, 370, *in camera*). Complaint Counsel did not deny that CX0451 was being offered for the truth of the matter asserted, *i.e.*, that the Social Security numbers for individuals listed in the Day Sheets were being used by other individuals, implying possible

[39] CLEAR (Consolidated Lead Evaluation and Reporting) is an investigative software database program, provided by Thompson Reuters, that is used by investigators at the FTC to obtain information on individuals and corporations. F. 214.

identity theft, but maintained that CX0451 was admissible because it has "sufficient indicia of reliability to be admitted" pursuant to Rule 3.43(b). (Tr. 369, *in camera*). To address Respondent's objection, Complaint Counsel was given the opportunity to lay a foundation for the reliability of CX0451, which it sought to do through the testimony of FTC investigator Kevin Wilmer.

As set forth in detail in Section II.E.4., *supra*, Mr. Wilmer was asked by Complaint Counsel to determine whether the nine digit numbers appearing in the Sacramento Documents, which he presumed to be Social Security numbers, had been used by people with different names. F. 217-218. To perform his task, Mr. Wilmer issued a "query" to the CLEAR database. F. 219. Mr. Wilmer testified that it was his "understanding" that the CLEAR database is an aggregation of information obtained from a variety of sources, including credit bureau information, utility information, information from civil judgments and criminal convictions, and other forms of publicly and privately available information. F. 214. Specifically, Mr. Wilmer copied each number that he believed to be a Social Security number and pasted the number onto a CLEAR-provided spreadsheet. F. 219. He then submitted the spreadsheet to CLEAR with a request that CLEAR use its "batching" function to query the CLEAR database, determine who used that apparent Social Security number, and return the information to him. F. 219. In response to Mr. Wilmer's CLEAR database query, CLEAR returned a spreadsheet containing the nine digit numbers that Mr. Wilmer entered, and CLEAR's data, drawn from its various sources, as to the names of people who had used that number as a Social Security number. F. 220. Mr. Wilmer identified CX0451 as the results returned to him by Thompson Reuters in response to his CLEAR database query, to which Mr. Wilmer added certain color-coding to differentiate the various names. F. 221.

After viewing proffered CX0451, hearing testimony from Mr. Wilmer, and considering the arguments of the parties, admission of CX0451 was denied on the ground that there was an insufficient foundation for determining the accuracy or reliability of the information in the CLEAR database, which provided the data for proffered CX0451. The ruling stated preliminarily: "I have concerns and I continue to have concerns about the reliability of the data comprising the spreadsheet [CX0451]. For example, I ruled earlier in this trial that I wouldn't allow sworn affidavits to be admitted into evidence. In this case, we are lacking even a sworn

statement or certification that the . . . CLEAR data is in fact accurate. And in fact, I have no idea if there's a . . . disclaimer on the Website stating that the information is not accurate." (Tr. 371, *in camera*). The ruling concluded that the foundation laid by Complaint Counsel was "wholly and totally lacking to make [CX0451] sufficiently reliable" to show that apparent Social Security numbers in the Sacramento Documents are being used by other people and therefore indicative of identity theft having occurred in this case. *See also* Tr. 371-372, *in camera* ("[W]e don't know if the Social Security number on the day sheet was correct [and w]e don't know if the Social Security number that the CLEAR data reflected was accurate. . . . [T]he source of [the CLEAR database] is from so many varied areas, real estate documents, utility bills, law enforcement records, criminal indictments, whatever, someone could easily type incorrectly one of the digits of a Social Security number.").

The record amply supports the denial of admission of proffered CX0451 as probative evidence of potential or actual identity theft from the exposure of the Sacramento Documents. The reliability of proffered CX0451 turns on the authenticity, accuracy, and/or reliability of the CLEAR database, and specifically, the data that is entered into the public and private databases from which the CLEAR database draws its information. However, Mr. Wilmer lacked sufficient knowledge of these matters. F. 224-226. In fact, Mr. Wilmer could not possibly authenticate or otherwise vouch for the reliability of the data in CX0451 since he has no personal knowledge of the CLEAR database itself, or the accuracy or reliability of the source data comprising the CLEAR database. F. 224-226. In addition, Mr. Wilmer, who had no connection to Thompson Reuters, which collects the source data upon which CX0451 is based, did not ask CLEAR to identify the source(s) of the data CLEAR used to populate the CLEAR spreadsheet, although he could have received this information if he had asked, because "that wasn't a part of [his] assignment." F. 224. Mr. Wilmer had no knowledge of, and did not ask CLEAR, whether some of the numbers reported by CLEAR had stemmed from bad keystrokes on the part of a reporting source, such as a bank. F. 225. Mr. Wilmer was not asked to determine any of the above, and was not asked to, and did not, contact any of the individuals listed in the Sacramento Documents. F. 226. In fact, Mr. Wilmer was not even asked to confirm that the nine digit numbers appearing on the Day Sheets in fact constituted Social Security numbers, or that the presumed Social Security numbers actually belonged to the associated names in the Sacramento Documents.

F. 217-218, 222. The spreadsheet offered as CX0451 does not indicate which individual associated with a Social Security number is the true owner of the number, if any.[40] F. 223.

Based on the failure to demonstrate the authenticity or reliability of the data returned by the CLEAR database, which is contained in proffered CX0451, the document cannot properly support any factual finding or any valid conclusion in this case. Moreover, even if proffered CX0451 were sufficiently reliable to be admitted, at best, proffered CX0451 shows only that individuals with different names are using the same Social Security number. However, on the record presented, this fact does not demonstrate or even imply that consumers in the Sacramento Documents are victims of identity theft. As noted above, there is no evidence that the individuals associated with Social Security numbers in the Sacramento Documents are the true owners of those Social Security numbers, and this fact cannot properly be assumed. Moreover, the evidence fails to show whether or not some of the people listed in the Sacramento Documents had voluntarily shared their personal information for others to use, or whether family members had taken their personal information without consent.

For all the foregoing reasons, Complaint Counsel has failed to prove the allegation in Complaint ¶ 21 that Social Security numbers in the Sacramento Documents "are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves," and Mr. Kam's opinions of likely identity theft from the Sacramento Documents, to the extent they rely on the assertion that Social Security numbers in the Sacramento Documents have been used by people with different names, are entitled to no weight.

ii. Mr. James Van Dyke

In support of its claim that the exposure of the Sacramento Documents is likely to cause substantial consumer injury, Complaint Counsel also relies on statistics reported in the 2013 Javelin Survey, also referenced in Section III.D.5.c.ii., *supra* regarding the 1718 File, that

[40] Indeed, even the relevance of CX0451 is questionable since Complaint Counsel failed to prove that the Sacramento Documents were even connected to Respondent's computer network security as alleged in the Complaint.

(1) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing new account fraud within the preceding 12 months, at an average consumer loss of $449; (2) 7.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing non-card fraud within the preceding 12 months, at an average consumer loss of $207; and (3) 13.1% of survey respondents who reported being notified within the 12 months preceding the survey that their SSN was disclosed in a data breach also reported experiencing existing card fraud with the preceding 12 months, at an average consumer cost of $106. CX0741 (Van Dyke Expert Report at 8-12). This evidence is unpersuasive, however. Mr. Van Dyke did not conduct a survey of the consumers listed in the Sacramento Documents. F. 256. The consumers whose Social Security numbers were exposed in the Sacramento Incident were notified of the incident in March 2013. F.212. If the assumptions underlying Complaint Counsel's theory of likely harm were to be believed and applied to this incident, then at least some of these consumers would have become victims of identity theft within 12 months. Yet, Complaint Counsel fails to identify even one consumer who suffered identify theft or identity fraud, within that 12 month period, or at any time thereafter. These facts undermine the persuasive value of Mr. Van Dyke's opinions and the assertion that harm is likely in this case.

e. Conclusion

For all the foregoing reasons, the evidence fails to prove that Respondent's alleged failure to reasonably secure the data on its computer network caused the exposure of the Sacramento Documents, or that this exposure has caused, or is likely to cause, substantial consumer harm.

7. Risk of Harm to Consumers whose Personal Information is Maintained on LabMD's Computer Network

a. Introduction

Complaint Counsel argues that LabMD's alleged failure to employ reasonable security practices "placed all consumers whose Personal Information is on [LabMD's computer] network at risk." CCB at 68. In support of this contention, Complaint Counsel points to opinions of its experts that the types of personal data kept by LabMD, such as names, Social Security numbers,

payment information, and health insurance information, "are the types of information needed to perpetrate frauds, and are the target of data thieves." CCB at 68. Therefore, Complaint Counsel concludes, the "risk of unauthorized exposure . . . is likely to cause" identity theft, medical identity theft, and other harms. CCB at 68. Put another way, Complaint Counsel argues that Respondent's alleged unreasonable data security creates an "elevated" or "increased" risk of an unauthorized disclosure, and that there is a "correlation" between being a data breach victim and being an identity theft victim; therefore, Respondent's alleged unreasonable data security is "likely to cause" consumers harm. CCCL 27.

Respondent contends that Complaint Counsel's position, based upon expert opinion, constitutes speculation about possible future identity theft, while the record is devoid of evidence of actual or likely identity theft, and does not satisfy Complaint Counsel's burden under Section 5(n) to prove that Respondent's alleged conduct caused or is likely to cause substantial consumer injury. Respondent further argues that Complaint Counsel's proffered consumer injury experts were not qualified to assess the risk posed by Respondent's alleged unreasonable data security, and that their opinions as to risk were based on assumptions and speculation.

As explained further below, Complaint Counsel's theory that harm is likely for all consumers whose Personal Information is maintained on LabMD's computer network, based on a "risk" of a future data breach and resulting identity theft injury, is without merit. First, the expert opinions upon which Complaint Counsel relies do not specify the degree of risk posed by Respondent's alleged unreasonable data security, or otherwise assess the probability that harm will result. To find "likely" injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture. Second, a "risk" of harm is inherent in the notion of "unreasonable" conduct. To allow unfair conduct liability to be based on a mere "risk" of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone. Such a holding would render the requirement of "likely" harm in Section 5(n) superfluous, and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," consumer harm.

b. Analysis

As framed by Complaint Counsel, the likelihood of substantial consumer injury to the consumers whose Personal Information is presently maintained on Respondent's computer network is based on the asserted risk that identity thieves, targeting the types of information held by LabMD, will successfully breach Respondent's computer network, take Personal Information, and misuse that information to commit identity theft harms. In the instant case, there is no evidence that this has happened in the past,[41] or that any consumer has suffered any harm as a result of Respondent's alleged unreasonable data security, including as a result of the alleged Security Incidents, as discussed above.

In *International Harvester*, upon which Complaint Counsel relies on the issue of risk (*see* CCCL 26), the Commission was required to assess the risk of consumer harm from certain safety defects in the respondent's tractors, to determine whether it was deceptive to fail to disclose such defects. "The implied warranty of fitness is not violated by all undisclosed safety problems. The critical issue is the degree of risk involved. . . . [A] seller impliedly warrants only that a product is reasonably safe, not that it is free of all hazards. We recognize that there is no such thing as a totally safe product, and especially not when dealing with relatively complex machinery." 1984 FTC LEXIS 2, at *252 and n.50. Similarly, as the Commission has acknowledged in this case, "[t]here is no such thing as perfect [computer] security." *LabMD*, 2014 FTC LEXIS 2, at *52. Accordingly, it was incumbent upon Complaint Counsel to demonstrate "the degree of risk involved." *See Int'l Harvester*, 1984 FTC LEXIS 2, at *252 and n.50. As the Commission stated in *International Harvester*, to suggest that there is a kind of risk that is separate from statistical risk "amounts really to no more than a conversational use of the term in the sense of 'at risk.' In this sense everyone is 'at risk' at every moment, with respect to every danger which may possibly occur. When divorced from any measure of the probability of occurrence,

[41] As noted above in Section III.D.6., the evidence fails to prove that the Sacramento Documents were obtained from a breach of Respondent's computer network security. In addition, as discussed above in Section III.D.5., while the 1718 File incident constituted a "data breach" in the broad sense of an unauthorized disclosure, the circumstances under which that disclosure occurred, through Tiversa's locating and downloading the 1718 File via peer-to-peer file sharing, are not analogous to the type of targeted intrusion of computer security by identity thieves posited by Complaint Counsel.

however, such a concept cannot lead to useable rules of liability." *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52.[42]

Judged against the principles for assessing risk set forth in *International Harvester*, the opinions of Complaint Counsel's experts, upon which Complaint Counsel relies, are insufficient because the experts failed to specify the degree of risk, or otherwise measure the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and identity theft injury. Mr. Kam opined generally that Respondent's asserted failure to reasonably protect its consumers' Personal Information poses an "increased" or "elevated" risk of unauthorized disclosure of this information, which "in turn is likely to cause" identity theft harm. CX0742 (Kam Expert Report at 10, 23). He based this opinion on the further broad opinion that cyber-criminals in general target healthcare organizations for attack, and that inadequate data security by such organizations renders their data security systems "vulnerable" to an attack by these criminals. *Id.* at 23; *see also* Kam, Tr. 558. *See* CCFF 1646-1649; 1653-1656. Mr. Kam "assumed" that Respondent's data security was unreasonable, and did not undertake to assess the degree of risk presented by Respondent's particular practices, or to assess the probability or likelihood that Respondent's computer network will be breached in the future. F. 244-245. Indeed, Mr. Kam has no expertise in computer network security, and therefore could not properly opine on the risk posed by Respondent's computer security, or on the probability or likelihood of a breach. *See* F. 9-10, 245. Mr. Kam's opinions as to a generalized increased risk of cyber-attack on healthcare organizations whose data security systems are "vulnerable" to such criminals is "divorced from any measure of the probability" of such an occurrence in this case. *See Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. Accordingly, Mr. Kam's opinion in this regard is not persuasive evidence that any or all the consumers whose Personal Information is maintained by LabMD on its computer network are "likely" to suffer harm.

The opinion offered by Complaint Counsel's other consumer harm expert, Mr. Van Dyke, also fails to assess the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and resulting harm. Mr. Van Dyke candidly admitted

[42] As noted above, as in *International Harvester*, risk is a critical issue for Complaint Counsel's claim. Accordingly, notwithstanding that the discussion of risk in *International Harvester* was in the context of a deception claim, as opposed to an unfair conduct claim, the Commission's framework for assessing risk is nevertheless instructive.

that he did not, and was not able to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except as to those that were listed on the 1718 File or in the Sacramento Documents. F. 258.

Moreover, Mr. Van Dyke's "risk" opinion is even more amorphous than that of Mr. Kam. Mr. Van Dyke states that, because consumer personal information in general is a "target of data thieves," LabMD's alleged unreasonable data security "risked exposing" consumers "to a likelihood" of harm. CX0741 (Van Dyke Expert Report at 12-13). Whatever the meaning of "likely" harm, as used in Section 5(n), surely it requires more than a mere "risk" of "an exposure" to "a likelihood" of harm. *See also* CCCL 30 (arguing that in "potentially exposing" consumers' Personal Information "to unauthorized disclosure," Respondent's conduct is "likely to cause injury . . ").

Furthermore, like Mr. Kam, Mr. Van Dyke did not assess Respondent's particular data security practices, having assumed that Respondent's data security was "unreasonable," F. 257, and his opinion is therefore also "divorced from any measure of the probability" that a data breach, and resulting identity theft harm, will occur in this case. *See Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. In addition, like Mr. Kam, Mr. Van Dyke is not qualified to assess Respondent's computer security. *See* F. 12-14.

The only expert proffered by Complaint Counsel who is arguably qualified to assess the degree of risk posed by Respondent's computer security practices, Dr. Raquel Hill, did not opine as to the probability or likelihood that Respondent's computer network would be breached, or whether Respondent's data security practices were likely to cause any consumer harm. When asked if she had an opinion as to the likelihood of consumer harm resulting from Respondent's asserted unreasonable data security, Dr. Hill responded that she did not form such an opinion; that she was instructed to assume that identity theft harm "could occur" *if* consumers' personal information on LabMD's network was exposed; and that she "assumed" that such harm was likely. F. 237. The likelihood of such an exposure, and resulting consumer harm, cannot properly be assumed. This assumption by the government's only witness who arguably could have opined on the specific risk or probability that Respondent's particular data security

practices will result in an unauthorized exposure – the logical prerequisite to any potential consumer harm – leaves virtually no evidence to support the contention that LabMD's alleged unreasonable security practices are likely to cause harm to consumers, simply because their Personal Information is maintained on Respondent's computer network.

Under the evidence presented, to conclude that consumers whose Personal Information is maintained on Respondent's computer network are "likely" to suffer a data breach and subsequent identity theft harm would require speculation upon speculation. Among other things, it would have to be assumed that, at some unknown point in the future, Respondent's computer system will be breached by a presently unknown third-party who, at some undetermined point thereafter, will use the stolen information to harm those consumers.[43] *Cf. Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3rd Cir. 2011) (finding alleged increased risk of future injury too attenuated for Article III standing purposes, even though there had been a prior security breach by an unknown hacker, because the likelihood of actual injury from the breach was "dependent on entirely speculative, future actions of an unknown third-party"). *See* Policy Statement, *supra*, at *307 (stating that injury must not be speculative); 1982 Policy Letter, *supra* (stating that Commission's resources should not be used for speculative harm).

Moreover, if an unspecified, theoretical "risk" of a future data breach and resulting identity theft were sufficient to prove unfair conduct in the instant case, then the clear requirement in Section 5(n) that injury be "likely" would be vitiated. Under common law negligence principles, which both parties cite in connection with the meaning of "unreasonableness" (CCCL 16; RCL 97),[44] "unreasonable" conduct, by definition, is conduct

[43] Complaint Counsel's argument as to the likelihood of future harm for all consumers whose Personal Information is maintained by LabMD is premised on the asserted vulnerability of LabMD's computer network to infiltration by identity thieves who would then commit identity crimes. To the extent Complaint Counsel also argues a likelihood of emotional or other privacy harms, allegedly arising from an unauthorized exposure of sensitive medical information alone, such subjective harm, unaccompanied by any tangible injury such as monetary harm or health and safety risks, would not constitute "substantial injury" within the meaning of Section 5(n).

[44] The Commission also referred to negligence standards as relevant to the "unreasonable data security" claim in the instant case. *LabMD*, 2014 FTC LEXIS 2, at *47-48. In rejecting LabMD's contention that charging LabMD with employing unreasonable data security in the absence of promulgated data security standards violated due process, the Commission stated: "LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself."

that exposes another to an unreasonable "risk" of harm. *See, e.g.*, Restatement (Second) of Torts § 298 (reasonable conduct is that which a reasonable person would recognize as necessary to prevent creating an unreasonable risk of harm); *see also id.* at § 291 ("Where an act is one which a reasonable man would recognize as involving a risk of harm to another, the risk is unreasonable and the act is negligent if the risk is of such magnitude as to outweigh what the law regards as the utility of the act or of the particular manner in which it is done."). Thus, to contend that proof of risk of injury – even an elevated or increased risk – is sufficient to prove "unfair" conduct is tantamount to arguing that "unreasonable" data security, by definition, is an unfair practice. This is contrary to the theory of the Complaint, which alleges both unreasonable data security and likely injury. Complaint ¶¶ 10, 22. *See also LabMD*, 2014 FTC LEXIS 2, at *52 (holding that unfair conduct liability in the area of data security requires proof of unreasonable data security *and* actual or likely resulting injury) (emphasis added). In addition, to base unfair conduct liability upon proof of unreasonable data security alone would, on the evidence presented in this case, effectively expand liability to cases involving generalized or theoretical "risks" of future injury, in clear contravention of Congress' intent, in enacting Section 5(n), to limit liability for unfair conduct to cases of actual or "likely" substantial consumer injury. *See, e.g.*, H.R. CONF. REP. 103-617, 1994 WL 385368, at *11-12, FTC Act Amendments of 1994 (noting that Section 5(n) is to *limit* unfair acts or practices under the reach of Section 5 to those that, *inter alia*, "cause or are likely to cause substantial injury to consumers") (emphasis added); *see also* S. REP. 103-130, 1993 WL 322671, at *4 ("This section amends section 5 of the FTC Act to limit unlawful 'unfair acts or practices' to *only* those which cause or are likely to cause substantial injury to consumers . . .") (emphasis added).

It is also significant that the Commission, in rejecting Respondent's argument that the unfair conduct claim in this case violated its due process rights to fair notice of what conduct was prohibited, specifically held that "the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n)," provided the required constitutional notice. *LabMD*, 2014 FTC LEXIS 2, at *46. That three-part statutory standard prohibits conduct that, *inter alia*, "causes or is likely to cause" substantial consumer injury. If unfair conduct liability can be premised on "unreasonable" data security alone, upon proof of a generalized, unspecified "risk" of a future data breach, without regard to the probability of its occurrence, and without

proof of actual or likely substantial consumer injury, then "the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n)," would not provide the required constitutional notice of what is prohibited.

Complaint Counsel asserts that Section 5 unfair conduct liability can be imposed based solely on the risk of a data breach and that proof of an actual data breach is not required. Transcript of Closing Arguments, Sept. 16, 2015, at 57. Fundamental fairness dictates that proof of likely substantial consumer injury under Section 5(n) requires proof of something more than an unspecified and hypothetical "risk" of future harm, as has been submitted in this case.[45]

c. Conclusion

Proof of a "risk" of harm, alone, "[w]hen divorced from any measure of the probability of occurrence, . . . cannot lead to useable rules of liability." *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. In the instant case, at best, Complaint Counsel's evidence of "risk" shows that a future data breach is possible, and that if such possible data breach were to occur, it is possible that identity theft harm would result. However, possible does not mean likely. Possible simply means not impossible. Such proof does not meet the minimum standard for declaring conduct "unfair" under Section 5 of the FTC Act, which requires that harm be "likely," and cannot lead to useable rules of liability. Accordingly, for all the foregoing reasons, the evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial injury to consumers whose Personal Information is maintained on LabMD's computer network.

E. CONCLUSION

Section 5(n) of the FTC Act provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the

[45] It should also be noted that Complaint Counsel's proffered data security expert, Dr. Hill, confined her opinions as to Respondent's alleged unreasonable data security to the time period from January 2005 through July 2010, referred to as the "Relevant Time Period." Thus, whatever risk might be inherent in Respondent's alleged "unreasonable" data security during the Relevant Time Period, the record is devoid of expert opinion as to the degree of risk beyond that period. Also, relevant to the assessment of risk in this case is that LabMD wound down its operations beginning in January 2014, and, as of May 2014, LabMD's operations were limited to maintaining tissue samples, and providing copies of prior test data to its physician clients only via facsimile. F. 36-39.

act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Accordingly, in the instant case, the burden was on Complaint Counsel to prove, initially, that Respondent's alleged failure to employ "reasonable and appropriate" data security "caused, or is likely to cause, substantial injury to consumers," as alleged in the Complaint. Complaint ¶¶ 10, 22. The evidence presented in this case fails to prove these allegations. As addressed in detail in this Initial Decision, there is no evidence that any consumer has suffered any substantial injury as a result of Respondent's alleged conduct, and both the quality and quantity of Complaint Counsel's evidence submitted to prove that such injury is, nevertheless, "likely" is unpersuasive. In reaching these conclusions the totality of the record evidence has been fully considered and weighed.

In summary, there is no evidence that any consumer has suffered any injury as a result of the 2008 exposure of the 1718 File, and the evidence fails to show that this exposure, to Tiversa, Professor Johnson, and the FTC, is likely to cause any substantial consumer injury. In addition, the evidence further fails to show that the Sacramento Documents were exposed in 2012 as a result of any alleged computer security failure of Respondent, or that the exposure of these documents has caused, or is likely to cause, any substantial consumer injury. Finally, the theory that, there is a likelihood of substantial injury for all consumers whose information is maintained on Respondent's computer networks, because there is a "risk" of a future data breach, is without merit because the evidence presented fails to demonstrate a likelihood that Respondent's computer network will be breached in the future and cause substantial consumer injury. While there may be proof of possible consumer harm, the evidence fails to demonstrate probable, *i.e.*, likely, substantial consumer injury.

Because the evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury, as required by Section 5(n) of the FTC Act, Respondent's alleged unreasonable data security cannot properly be declared an unfair act or practice in violation of Section 5(a) of the FTC Act. Accordingly, the Complaint must be DISMISSED.

IV. SUMMARY OF CONCLUSIONS OF LAW

1. Section 5 of the FTC Act grants the FTC the authority over "unfair or deceptive acts or practices in or affecting commerce" by "persons, partnerships, or corporations . . . ." 15 U.S.C. § 45(a)(1)-(2).

2. Respondent is a corporation within the meaning of Sections 4 and 5 of the FTC Act. 15 U.S.C. §§ 44, 45.

3. The acts and practices alleged in the Complaint are "in or affecting commerce" under the FTC Act. 15 U.S.C. § 45(a)(1).

4. Complaint Counsel bears the burden of proving the allegations of the Complaint that Respondent engaged in unfair conduct in violation of Section 5(a) of the FTC Act by a preponderance of evidence.

5. Section 5(n) of the FTC Act provides that "[t]he Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

6. Complaint Counsel bears the burden of proving by a preponderance of the evidence the allegations of the Complaint that Respondent's failure to provide "reasonable and appropriate" security for personal information maintained on LabMD's computer networks, "caused or is likely to cause" substantial consumer injury that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

7. Congress amended the FTC Act in 1994 to add Section 5(n). Congress' intent in adding Section 5(n) to the FTC Act was to establish an outer limit to the Commission's authority to declare an act or practice unfair.

8. Section 5(n) of the FTC Act is a three-part test, and all three parts must be proven before an act or practice can be declared "unfair."

9. The three-part test in Section 5(n) was intended to codify, as a statutory limitation on unfair acts or practices, the principles of the FTC's December 17, 1980 policy statement on unfairness, reaffirmed by a letter from the FTC dated March 5, 1982, in order to provide guidance and to prevent a future FTC from abandoning those principles.

10. Actual or likely substantial consumer injury, which is also not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to

consumers or to competition, is a legal precondition to finding a respondent liable for unfair conduct.

11. Unjustified consumer injury is the primary focus of the FTC Act.

12. The Commission has stated that its "concerns should be with substantial consumer injuries; its resources should not be used for trivial or speculative harm."

13. Consumer injury may be "substantial" under Section 5(n) if a relatively small harm is inflicted on a large number of consumers or if a greater harm is inflicted on a relatively small number of consumers.

14. In most cases, substantial consumer injury involves monetary or economic harm or unwarranted health and safety risks.

15. Unfair conduct cases usually involve actual and completed harms.

16. Historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm.

17. Complaint Counsel bears the burden of proving, initially, that Respondent's alleged failure to employ "reasonable and appropriate" data security "caused, or is likely to cause, substantial injury to consumers," as alleged in the Complaint.

18. Complaint Counsel has failed to meet its burden of proving that Respondent's alleged unreasonable data security caused substantial consumer injury. The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged conduct.

19. Section 5(n) does not define the meaning of "likely" injury. Where a statute does not define a term, it is construed in accordance with its ordinary meaning.

20. The Merriam-Webster dictionary states that "likely" is "used to indicate the chance that something will happen," and is primarily defined as "having a high probability of occurring or being true."

21. The Commission has interpreted its deception standard, which requires proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ."

22. The term "likely" in Section 5(n) does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur.

23. Complaint Counsel has failed to meet its burden of proving that Respondent's alleged unreasonable data security is "likely to cause" substantial consumer injury. There

may be proof of possible consumer harm, but the evidence fails to demonstrate probable, *i.e.*, likely, substantial consumer injury.

24. Complaint Counsel has failed to prove that the 2008 exposure of the 1718 File caused, or is likely to cause, any substantial consumer injury.

25. Subjective feelings of harm, such as embarrassment, upset, or stigma, standing alone, without accompanying, clearly demonstrated, tangible injury, do not constitute "substantial injury" within the meaning of Section 5(n).

26. Evidence in the record provided by Tiversa and its chief executive officer and corporate designee Mr. Robert Boback, claiming that Tiversa found the 1718 File in "multiple locations" on peer-to-peer networks, including at IP addresses belonging to suspected or known identity thieves, is entitled to no weight. Such evidence, including without limitation, Mr. Boback's 2013 discovery deposition, Mr. Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, is unreliable, not credible, and outweighed by credible contrary testimony from Mr. Richard Wallace.

27. Complaint Counsel has failed to prove that Respondent's alleged failure to reasonably secure data on its computer network caused, or is likely to cause, substantial injury to consumers due to the exposure of the Sacramento Documents because Complaint Counsel has failed to prove that the Sacramento Documents were maintained on Respondent's computer network.

28. Complaint Counsel has failed to prove that the Sacramento Documents were exposed in 2012 as a result of any alleged computer security failure of Respondent.

29. Even if there were a causal connection between Respondent's computer network and the exposure of the Sacramento Documents, Complaint Counsel has failed to prove that the exposure of these documents has caused, or is likely to cause, any substantial consumer injury.

30. Complaint Counsel has failed to prove the allegation in Complaint ¶ 21 that Social Security numbers in the Sacramento Documents "are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves," because the evidence upon which Complaint Counsel relies (proffered exhibit CX0451) is unreliable and entitled to no weight.

31. Complaint Counsel's assertion that there is a likelihood of substantial injury for all consumers whose information is maintained on Respondent's computer networks, regardless of whether their information has been exposed, on the theory that there is a "risk" of a future data breach, is without merit because Complaint Counsel has failed to prove the likelihood that Respondent's computer network will be breached in the future and cause substantial consumer injury.

32. To suggest that there is a kind of risk that is separate from statistical risk amounts to no more than a conversational use of the term "risk." Proof of a "risk" of harm alone, when divorced from any measure of the probability of occurrence, cannot lead to useable rules of liability.

33. To find "likely" substantial consumer injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture.

34. To allow unfair conduct liability to be based on proof of a generalized "risk" of harm alone – even an elevated or increased risk – without regard to the probability that such harm will occur would vitiate the requirement in Section 5(n) that substantial consumer injury be proven "likely" and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," substantial consumer injury.

35. Proof of likely substantial consumer injury under Section 5(n) requires proof of something more than an unspecified and hypothetical "risk" of future harm.

36. Based on the totality of the evidence presented, Complaint Counsel has failed to meet its burden of proving, by a preponderance of the evidence, that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury.

37. Because Complaint Counsel failed to meet its burden of proving the first prong of the three-part test in Section 5(n) – that Respondent's conduct caused, or is likely to cause, substantial consumer injury – Respondent's alleged failure to employ "reasonable and appropriate data security" for information maintained on its computer networks cannot be declared an "unfair" act or practice in violation of Section 5(a) of the FTC Act.

ORDER

For the reasons stated above, IT IS ORDERED that the Complaint be, and hereby is, DISMISSED.

ORDERED:

_____
D. Michael Chappell
Chief Administrative Law Judge

Date: November 13, 2015

EXHIBIT 21

PUBLIC

COPY

OFFICIAL TRANSCRIPT PROCEEDING

FEDERAL TRADE COMMISSION

DOCKET NO. 9357

TITLE LABMD, INC.

PLACE FEDERAL TRADE COMMISSION
600 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC

DATE SEPTEMBER 25, 2013

PAGES 1 THROUGH 39

INITIAL PRETRIAL CONFERENCE

FOR THE RECORD, INC.
10760 DEMARR ROAD
WHITE PLAINS, MD 20695
(301)870-8025

---

1 depending on the information. For example, financial
2 information has been misused to open new -- to conduct
3 credit card fraud and to go into bank accounts; and
4 medical information has been misused to steal insurance
5 benefits. In each of the last ten years, identity theft
6 has been the number one complaint that the FTC has
7 received. There were 369,000 complaints in 2012.
8 The personal information that LabMD maintains is
9 information that identity thieves want. This was action
10 was brought under Section 5 of the FTC Act. Section 5
11 provides the Commission with broad authority to address
12 new areas and practices as they develop.
13 JUDGE CHAPPELL: Have you -- in that regard, has
14 the Commission issued guidelines for companies to
15 utilize to protect this information or is there
16 something out there for a company to look to?
17 MR. SHEER: There is nothing out there for a
18 company to look to. The Commission has entered into
19 almost 57 negotiations and consent agreements that set
20 out a series of vulnerabilities that firms should be
21 aware of, as well as the method by which the Commission
22 assesses reasonableness.
23 In addition, there have been public statements
24 made by the Commission, as well as educational materials
25 that have been provided. And in addition, the industry,

1 the IT industry itself, has issued a tremendous number
2 of guidance pieces and other pieces that basically set
3 out the same methodology that the Commission is
4 following in deciding reasonableness, with one
5 exception, and the exception is that the Commission's
6 process as to the calculation of the potential consumer
7 harm from unauthorized disclosure of information.
8 JUDGE CHAPPELL: Is there a rulemaking going on
9 at this time or are there rules that have been issued in
10 this area?
11 MR. SHEER: There are no -- there is no
12 rulemaking, and no rules have been issued, other than
13 the rule issued with regard to the Gramm-Leach-Bliley
14 Act. There is a safeguards rule there which is issued
15 for financial institutions. The way that rule reads and
16 the way it works, it basically --
17 JUDGE CHAPPELL: The FTC has jurisdiction in
18 that area?
19 MR. SHEER: It has jurisdiction over certain
20 types of financial institutions, such as --
21 JUDGE CHAPPELL: Is that expressed in that Act?
22 MR. SHEER: It is.
23 JUDGE CHAPPELL: Okay.
24 MR. SHEER: As I was saying, Your Honor,
25 information security, which is an essential part of our

1 network. The company's security practices created
2 vulnerabilities an outsider could stitch together to
3 find a way into the network, to move around the network
4 and explore it, to find sensitive information, and then
5 to package up the information and export it from the
6 network without the company's noticing.
7 LabMD failed to implement reasonable security
8 measures, and that is an unfair act or practice because
9 it caused or is likely to cause substantial consumer
10 injury that's not offset by countervailing benefits to
11 consumers or competition and also not reasonably
12 avoidable by consumers. After all, how can a consumer
13 even know what LabMD's security practices were, let
14 alone assess how adequate or inadequate they might be?
15 One final point. Neither the complaint nor the
16 notice order prescribes specific security practices that
17 LabMD should implement going forward. They do not, for
18 example, require that a certain vulnerability scanning
19 product be used. Because security threats and responses
20 change so rapidly, the order leaves it to the company to
21 determine the particular security measures that, taken
22 together, will provide reasonable security at lowest
23 cost in its circumstances.
24 Although the Commission retains the right to do
25 so, under the notice order and all of the other

1 Commission information security consent orders, a strong
2 indication that security is reasonable is a security
3 certification from an independent IT professional who's
4 capable of balancing the costs and benefits and follows
5 protocols commonly used in the profession. These are
6 the same sorts of things that internal IT employees
7 commonly do for companies across the country. Frankly,
8 the order only asks LabMD to do what it should have been
9 doing anyway but didn't.
10 Thank you.
11 JUDGE CHAPPELL: I have one question. I heard
12 you refer to Section 5, but I also heard you refer to
13 various other rules, regulations, et cetera. Is it the
14 Government's position that whatever rule or regulation
15 or statute that you're alleging was violated is
16 contained within the four corners of this complaint?
17 MR. SHEER: What we're saying is that the
18 allegation is that the company failed to comply with
19 Section 5 in engaging an unfair act or practice by
20 failing to provide reasonable security for sensitive
21 information. We are saying that reasonableness is a
22 common sense balancing of cost and benefit and that
23 common sense is available from many, many sources,
24 including organizations -- government organizations,
25 such as the National Institute of Standards and

1 Technology, private entities, such as the SANS
2 Institute, and many others as well. So that we are
3 assessing reasonable -- reasonableness in much the same
4 way, following the same process that is commonly used
5 throughout the IT industry now. We add only one
6 additional factor, and that is take into account the
7 potential consumer harm from failing to have reasonable
8 security to protect that information.
9 JUDGE CHAPPELL: I'm not sure you answered my
10 question, Counselor. Are there any rules or regulations
11 that you're going to allege were violated here that are
12 not within the four corners of the complaint?
13 MR. SHEER: I misunderstood. I'm sorry. No.
14 JUDGE CHAPPELL: All right. Thank you.
15 MR. RUBINSTEIN: The facts in this case are
16 pretty simple and pretty clear. The billing manager,
17 the person responsible for handling LabMD's invoicing --
18 a small company, a very limited staff --
19 JUDGE CHAPPELL: Tell me more about what LabMD
20 does. Do you take blood samples?
21 MR. RUBINSTEIN: It's a pathology lab. The
22 customers -- LabMD's customers are doctors. You go in
23 to see a doctor -- and it's a very small specialty
24 business for particular kinds of cancer detection. You
25 go in to see a doctor. He will take a tissue sample for

EXHIBIT 22

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**

ORDER DENYING RESPONDENT LABMD'S MOTION TO DISMISS

By Commissioner Joshua D. Wright, for a unanimous Commission:[1]

This case presents fundamental questions about the authority of the Federal Trade Commission ("FTC" or "the Commission") to protect consumers from harmful business practices in the increasingly important field of data security. In our interconnected and data-driven economy, businesses are collecting more personal information about their customers and other individuals than ever before. Companies store this information in digital form on their computer systems and networks, and often transact business by transmitting and receiving such data over the Internet and other public networks. This creates a fertile environment for hackers and others to exploit computer system vulnerabilities, covertly obtain access to consumers' financial, medical, and other sensitive information, and potentially misuse it in ways that can inflict serious harms on consumers. Businesses that store, transmit, and use consumer information can, however, implement safeguards to reduce the likelihood of data breaches and help prevent sensitive consumer data from falling into the wrong hands.

Respondent LabMD, Inc. ("LabMD") has moved to dismiss the Complaint in this adjudicatory proceeding, arguing that the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the Federal Trade Commission Act ("FTC Act" or "the Act"), 15 U.S.C. § 45(a)(1). This view, if accepted, would greatly restrict the Commission's ability to protect consumers from unwanted privacy intrusions, fraudulent misuse of their personal information, or even identity theft that may result from businesses' failure to establish and maintain reasonable and appropriate data security measures. The Commission would be unable to hold a business accountable for its conduct, even if its data security program is so inadequate that it "causes or is likely to cause

[1] Commissioner Brill did not take part in the consideration or decision herein.

substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [such injury is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings ("Motion to Dismiss" or "Motion"), filed November 12, 2013, calls on the Commission to decide whether the FTC Act's prohibition of "unfair . . . acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does. We also reject LabMD's contention that, by enacting the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security, Congress has implicitly stripped the Commission of authority to enforce Section 5 of the FTC Act in the field of data security, despite the absence of any express statutory language to that effect. Nor can we accept the premise underlying LabMD's "due process" arguments – that, in effect, companies are free to violate the FTC Act's prohibition of "unfair . . . acts or practices" without fear of enforcement actions by the Commission, unless the Commission has first adopted regulations. Accordingly, we deny LabMD's Motion to Dismiss.

PROCEDURAL BACKGROUND

On August 28, 2013, the Commission issued an administrative complaint ("Complaint") against LabMD, a Georgia-based company in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers. The Complaint alleges that LabMD engaged in "practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks," *see* Complaint, ¶ 10; that these practices caused harm to consumers, including exposure to identity theft and disclosure of sensitive, private medical information, *id.*, ¶¶ 12, 17-21; and, consequently, that LabMD engaged in "unfair . . . acts or practices" in violation of the FTC Act. *Id.*, ¶¶ 22-23. LabMD submitted its Answer and Affirmative Defenses to the Administrative Complaint ("Answer") on September 17, 2013.

LabMD filed its Motion to Dismiss on November 12, 2013.[2] On November 22, 2013, Complaint Counsel filed its Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice ("CC Opp."). LabMD filed its Reply to Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss ("Reply") on December 2, 2013. Factual discovery is now underway and is scheduled to close on March 5, 2014. The evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014.

[2] The Commission issued an Order on December 13, 2013, denying both LabMD's request for a stay of the administrative proceedings pending resolution of its Motion to Dismiss (*see* Motion at 29-30) and a separate Motion for Stay Pending Judicial Review that LabMD filed on November 26, 2013.

STANDARD OF REVIEW

We review LabMD's Motion to Dismiss using the standards a reviewing court would apply in assessing a motion to dismiss for failure to state a claim.[3] *See* Fed. R. Civ. P. 12(b)(6); *see also* Motion at 8; CC Opp. at 3; *S.C. State Bd. of Dentistry*, 138 F.T.C. 230, 232-33 (2004); *Union Oil Co.*, 138 F.T.C. 1, 16 (2004). Under this framework, "[o]ur task is to determine whether the [Complaint] contains sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2010) (citation omitted). For purposes of this analysis, we "accept[] the allegations in the complaint as true and constru[e] them in the light most favorable to [Complaint Counsel]." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1288 (11th Cir. 2010).

ANALYSIS

I. THE COMMISSION HAS AUTHORITY TO ENFORCE THE FTC ACT BY ADJUDICATING WHETHER THE DATA SECURITY PRACTICES ALLEGED IN THE COMPLAINT ARE "UNFAIR."

LabMD contends that the Commission lacks statutory authority to regulate or bring enforcement action with respect to the data security practices alleged. Motion at 9-21. We disagree. As discussed below, the Commission's authority to protect consumers from unfair practices relating to deficient data security measures is well-supported by the FTC Act, is fully consistent with other statutes, and is confirmed by extensive case law.[4]

A. Congress Intended to Delegate Broad Authority to the Commission to Proscribe Activities that Qualify as "Unfair Acts or Practices."

LabMD's broadest argument is that Section 5 does not authorize the FTC to address *any* data security practices. *See, e.g.*, Motion at 10 ("even if Section 5 does authorize the FTC to

---

[3] The Commission's administrative adjudicatory proceedings are governed by the FTC Act and the Commission's Rules of Practice, rather than the rules and standards that govern federal courts. Nonetheless, "since many adjudicative rules are derived from the Federal Rules of Civil Procedure, the latter may be consulted for guidance and interpretation of Commission rules where no other authority exists." FTC Op. Manual § 10.7. Here, the most relevant provision in the Commission's Rules of Practice (16 C.F.R. § 3.11(b)(2)) is very similar to the analogous court rule (Fed. R. Civ. P. 8(a)(2)). Thus, in this instance, we exercise our discretion to apply the pleading standards summarized above.

[4] At some points in the Motion, LabMD frames its arguments as challenges to the scope of the Commission's "jurisdiction" (*e.g.*, at 1, 2, 8, 16, 18, 19), while elsewhere it acknowledges the Commission's "Section 5 'unfairness' authority" but asserts that we cannot apply such authority to LabMD's data security practices. *Id.* at 18. As the Supreme Court recently clarified, "there is *no difference*, insofar as the validity of agency action is concerned, between an agency's exceeding the scope of its authority (its 'jurisdiction') and its exceeding authorized application of authority that it unquestionably has." *City of Arlington v. FCC*, 133 S. Ct. 1863, 1870 (2013). This is because, "for agencies charged with administering congressional statutes[,] [b]oth their power to act and how they are to act is authoritatively prescribed by Congress." *Id.* at 1869; *see* Motion at 9.

regulate data-security, which it does not"); *id.* at 17 (asserting "the Commission's lack of power to regulate data security through its general Section 5 'unfairness' authority'"). Motion at 16. LabMD points out that "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate . . . data-security practices." *Id.* at 20. Ignoring the facially broad reach of Section 5's prohibition of "unfair . . . acts or practices in or affecting commerce," LabMD urges the Commission to conclude from the absence of explicit "data security" authority in the FTC Act that the Commission has no such authority. *See, e.g.,* Motion at 14 ("When Congress has wanted the FTC to have data security authority, it has said so"); *id.* ("However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope."); *id.* at 16 ("Section 5 does not give the FTC the authority to regulate data-security practices as 'unfair' acts or practices"); *id.* at 21 ("Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's [authority over] data security"). The statutory text, legislative history, and nearly a century of case law refute LabMD's argument.

As the courts have long recognized, "[n]either the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). Rather, the legislative history of the FTC Act confirms that Congress decided to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply. . . . There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (quoting S. Rep. No. 597, 63d Cong., 2d Sess., 13 (1914), and H.R. Conf. Rep. No.1142, 63d Cong., 2d Sess., 19 (1914)). *See also Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) (Congress "intentionally left development of the term 'unfair' to the Commission rather than attempting to define 'the many and variable unfair practices which prevail in commerce.'") (quoting S. Rep. No. 592, 63d Cong., 2d Sess., 13 (1914)).

This legislative history pertains to Congress' enactment of the prohibition of "unfair methods of competition" in 1914. Similar considerations motivated Congress's reuse of the same broad term ("unfair") when it amended the statute in 1938 to proscribe "unfair and deceptive acts and practices" as well as "unfair methods of competition." The 1938 amendment perpetuated and expanded the broad congressional delegation of authority to the Commission by "overturn[ing] . . . attempts [in some court decisions] to narrowly circumscribe the FTC's authority." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). Congress thus clarified that "the Commission can prevent such acts or practices which injuriously affect the general public as well as those which are unfair to competitors." *Id.* (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)).

As LabMD points out (*see* Motion at 18), Congress enacted legislation in 1994 that provided a sharper focus for the application of the Commission's "unfairness" authority, by amending the FTC Act to incorporate three specific criteria governing the application of "unfair . . . acts or practices" in adjudicatory and rulemaking proceedings. Specifically, the new Section 5(n) of the Act provides that, in enforcement actions or rulemaking proceedings, the Commission has authority to determine that an act or practice is "unfair" if that act or practice

"[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. 45(n). These criteria, derived from the Commission's pre-existing *Policy Statement on Unfairness*, codified the analytical framework that the Commission already had been applying for the preceding decade in its efforts to combat "unfair . . . acts or practices." *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("*Policy Statement on Unfairness*"), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984). Section 5(n)'s specific criteria provide greater certainty for businesses by setting forth the factors to be used to evaluate whether their acts or practices are "unfair." That fact alone refutes LabMD's contention that the "general statutory terms" in Section 5 are too "vague" to be applied to the conduct alleged in the Complaint. *See* Motion at 19.

At the same time, Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as "unfair." Thus, to this day, "Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis." *Am. Fin. Servs. Ass'n*, 767 F.2d at 966.

The Commission and the federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though – like the data security practices alleged in this case – "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices (*see* Motion at 20). *See, e.g., FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating and delivering unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364 (11th Cir.1988) (unilateral breach of standardized service contracts); *Am. Fin. Servs. Ass'n*, 767 F.2d at 971 (oppressive litigation conduct to repossess household goods sold on credit).

LabMD cites *American Bar Association v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), for the proposition that the Commission is overstepping the bounds of its authority to interpret the FTC Act. *See* Motion at 20. But that case is inapposite. *ABA* concerned the agency's determination, in construing the Gramm-Leach-Bliley Act ("GLB Act"), that attorneys fell within that statute's definition of "financial institutions" – a defined term that, in turn, incorporated by reference a set of lengthy and detailed definitions imported from other statutes and other agencies' regulations. The court found it "difficult to believe" that, in enacting a statutory "scheme of the length, detail, and intricacy of the one" under review, Congress could have left sufficient remaining ambiguity, "hidden beneath an incredibly deep mound of specificity," to support imposing GLB Act requirements upon "a profession never before regulated by federal [financial service] regulators, and never mentioned in the statute." 430 F.3d at 469. By contrast, the statutory text at issue in this case – "unfair . . . acts or practices" – conveys a far broader scope of interpretive flexibility, particularly given that this term is at the core of the Commission's own organic statute, the FTC Act.

LabMD similarly invokes *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), for the proposition that "simple 'common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude' . . . reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint." Motion at 19 (quoting *Brown & Williamson*, 529 U.S. at 133). But *Brown & Williamson* is inapposite as well. In that case, the Court found that the Food and Drug Administration's attempts to regulate tobacco products conflicted directly with concrete manifestations of congressional intent. In particular, the Court concluded that, if the FDA had the authority it claimed, its own findings would have compelled it to ban tobacco products outright, whereas various tobacco-related statutes made clear that Congress wished *not* to ban such products. *See* 529 U.S. at 137-39. Here, of course, LabMD can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers.

Similarly, the Court found that "Congress' specific intent when it enacted the FDCA" (Food, Drug & Cosmetics Act) in 1938 was to deny the FDA authority to regulate tobacco products. 529 U.S. at 146. The Court reasoned that, "*given the economic and political significance of the tobacco industry at the time*, it is extremely unlikely that Congress could have intended to place tobacco within the ambit of the FDCA absent any discussion of the matter." *Id.* at 147 (emphasis added).[5] By contrast, when enacting the FTC Act in 1914 and amending it in 1938, Congress had no way of anticipating the "economic and political significance" of data security practices in today's online environment. Accordingly, the fact that "there is no evidence in the text of the [FTC Act] or its legislative history that Congress in 1938 even considered the applicability of the Act" to data security practices is completely irrelevant. Congress could not possibly have had any "specific intent" to deny the FTC authority over data security practices. It did, however, intend to delegate broad authority to the FTC to address emerging business practices – including those that were unforeseeable when the statute was enacted. That is the only congressional intent that matters here.

B. The Commission Has Consistently Affirmed Its Authority under the FTC Act to Take Enforcement Action against Unreasonable Data Security Activities that Qualify as Unfair Acts and Practices

LabMD similarly attempts to draw support from the *Brown & Williamson* Court's determination that the FDA's 1996 "assertion of authority to regulate tobacco products" contradicted the agency's previous "consistent and repeated statements [over the preceding 73 years] that it lacked authority . . . to regulate tobacco absent claims of therapeutic benefit by the manufacturer," and the Court's conclusion that congressional enactments "against the backdrop" of the FDA's historic disavowal of authority confirmed that Congress did not intend to authorize such regulation. 529 U.S. at 132, 144-46. LabMD argues, by analogy, that "the Commission

[5] As the D.C. Circuit has recently recognized, these considerations are essential to the holding of *Brown & Williamson*, and, in their absence, that case does not justify restricting agency action under a broad statutory mandate. *See Verizon v. FCC*, No. 11-1355, at 23-25 (D.C. Cir., Jan. 14, 2014) (slip op.).

[previously] did not claim Section 5 'unfairness' authority to regulate patient-information (or any other) data-security practices," but "recently reversed course without explanation," thus purportedly defying congressional intent. Motion at 16, 18.

That analogy, too, is without merit. Unlike the FDA, the Commission has never disavowed authority over online privacy or data security matters. To the contrary, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and has repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5. *See* FTC Report to Congress, *Privacy Online*, at 2 (June 1998) ("*1998 Online Privacy Report*").[6] LabMD cites out-of-context snippets from the Commission's 1998 and 2000 reports to Congress for the unfounded proposition that, at that time, the Commission believed its authority over data security matters was "limited to ensuring that Web sites follow their stated information practices."[7] LabMD's characterization does not withstand scrutiny. Neither the text it quotes nor the reports as a whole can plausibly be read as disavowing the Commission's authority to take enforcement action against data security practices that violate Section 5's prohibition of "unfair . . . acts or practices," as defined in Section 5(n). Indeed, the Commission clearly stated that certain conduct relating to online data security is "likely to be an unfair practice," and, in both reports, confirmed its view that the FTC Act "provides a basis for government enforcement" against information practices [that] may be inherently . . . unfair, regardless of whether the entity has publicly adopted any fair information practice policies."[8] In context, the sentences from the 1998 and 2000 reports relied upon by LabMD simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children's online privacy) and that expanded rulemaking authority and enforcement remedies could enhance the Commission's ability to meaningfully address a broader range of such concerns.[9] The same

---

[6] *See* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[7] Motion at 16 n.12 (quoting *1998 Online Privacy Report* at 41) ("As a general matter, the Commission lacks authority to require firms to adopt information practice policies."); Reply at 7-8 (quoting FTC Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Age* (May 2000) ("*2000 Online Privacy Report*") (http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf) ("As a general matter, . . . the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites").

[8] *1998 Online Privacy Report* at 12-13, 40-41. *See also 2000 Online Privacy Report* at 33-34 ("The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5[,]" which "prohibits unfair and deceptive practices in and affecting commerce," and thus "authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain [norms concerning] fair information practices").

[9] *See 1998 Online Privacy Report* at 42 (recognizing that "Section 5 may only have application to some but not all practices that raise concern about the online collection and use of information from children," and recommending legislation authorizing the Commission to promulgate "standards of practice governing the online collection and use of information from children."); *2000 Online Privacy Report* at

error infects LabMD's mischaracterization of testimony that Commissioners and high-level Commission staff members delivered to various congressional committees and subcommittees.[10]

Since the late 1990s, the Commission has repeatedly affirmed its authority to take action against unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5, in reports, testimony to Congress, and other publicly-released documents.[11] The Commission has also confirmed this view by bringing administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal information collected from consumers online. For example, on May 1, 2006, the Commission filed a complaint in the U.S. District Court for the District of Wyoming, charging that defendant Accusearch, Inc. and its principal obtained consumers' private information (specifically, data concerning their telecommunications usage) and caused such data to be disclosed to unauthorized third parties without consumers' knowledge or consent. *FTC v. Accusearch, Inc.*, Case No. 2:06-cv-0105, Complaint, at ¶¶ 9-13. The Commission alleged that this conduct was "an unfair practice in violation of Section 5(a) of the FTC Act," *id.*, ¶ 14, because it "caused or [was] likely to cause substantial injury to consumers that [was] not reasonably avoidable by consumers and [was] not outweighed by

---

36-37 (seeking legislation granting "authority to promulgate more detailed standards pursuant to the Administrative Procedure Act," including "rules or regulations [that] could provide further guidance to Web sites by defining fair information practices with greater specificity[,]"such as "what constitutes 'reasonable access' and 'adequate security'"). *See also* Motion at 17 n.13 (quoting same).

[10] *See* Motion at 16-17, nn.12, 13, 14 (citing testimony by Chairman Robert Pitofsky in 1998, then-Commissioner Edith Ramirez in 2011, Chairman Jonathan Leibowitz in 2012, and Bureau Directors Eileen Harrington and David Vladeck in 2009 and 2011, respectively). In such testimony, the FTC representatives conveyed the Commission's support for draft data security legislation that would expand the FTC's *existing* authority by providing it with rulemaking authority under the Administrative Procedure Act and civil penalty authority. *See, e.g.*, Prepared Statement of the FTC, *Data Security*, presented by Commissioner Edith Ramirez to House Comm. on Energy & Commerce, Subcomm. on Commerce, Mfg., and Trade, at 11-12 (June 5, 2011) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf).

[11] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Innovative Solutions for an Evolving Problem*, presented by Bureau Dir. Lydia B. Parnes to Senate Comm. on the Judiciary, Subcomm. on Terrorism, Tech., and Homeland Security, at 5-6 (Mar. 21, 2007) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-identity-theft-innovative-solutions-evolving-problem/p065409identitytheftsenate03212007.pdf); FTC Staff Report, *Protecting Consumers in the Next Tech-ade*, at 29-30 (Spring 2008) (http://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-next-tech-ade-report-staff-federal-trade-commission/p064101tech.pdf); FTC Report, *Security in Numbers, SSNs and ID Theft*, at 7 (Dec. 2008) (http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf); Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*, presented by Assoc. Bureau Dir. Maneesha Mithal to House Comm. on Ways and Means, Subcomm. on Soc. Security, at 8 (April 13, 2011) (http://ftc.gov/os/testimony/110411ssn-idtheft.pdf); FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 14, 73 (March 26, 2012) (http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers). *See also* note 13, *infra*.

countervailing benefits to consumers or competition." *Id.*, ¶ 13. The district court agreed, granting summary judgment to the Commission in 2007, and the Tenth Circuit affirmed in 2009. *See Accusearch*, *supra*, 570 F.3d 1187. Since then, the Commission has taken the same position in dozens of other enforcement proceedings, including administrative adjudications,[12] as well as complaints filed in federal courts, *see* CC Opp. at 12-13 n.9 (citing cases). In these cases, the Commission challenged allegedly unreasonable data security measures (or other practices that enabled unauthorized third parties to harm consumers by obtaining access to their confidential personal data) as "unfair acts or practices" in violation of Section 5. And in each case, it clearly reaffirmed its position that it possessed jurisdiction over the allegedly "unfair" data security practices under Section 5.

The fact that the Commission initially focused its enforcement efforts primarily on "deceptive" data security practices, and began pursuing "unfair" practices in 2005, does not mean that the Commission lacked jurisdiction over "unfair" practices before then. As then-Commissioner Orson Swindle testified to a House subcommittee in 2004, "To date, the Commission's security cases have been based on its authority to prevent deceptive practices," but it "also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'"[13] LabMD cites Commissioner Swindle's reference to the Commission's "deceptiveness" authority over data security practices, *see* Motion at 16 n.12, but neglects to mention his reference to the Commission's "unfairness" authority over such practices.

LabMD also misinterprets the Commission's expressions of support for legislation relating to data security as requests for authority to fill regulatory "gaps" that it could not fill without such legislation. *Id.* at 17 & nn.13, 14. LabMD refers to three data security-related laws that the Commission supported, and that Congress ultimately enacted – *i.e.*, the GLB Act,[14] the

---

[12] *See BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 470 (2005); *DSW, Inc.*, 141 F.T.C. 117, 122 (2006); *CardSystems Solutions, Inc.*, Docket No. C-4168, 2006 WL 2709787, *3 (Sept. 5, 2006); *Reed Elsevier, Inc.*, Docket No. C-4226, 2008 WL 3150420, *4 (July 29, 2008); *TJX Cos., Inc.*, Docket No. C-4227, 2008 WL 3150421, *3 (Sept. 29, 2008). In these and similar cases, the Commission issues its final Decisions & Orders only after placing the relevant proposed consent orders on the public record, issuing Notices in the Federal Register that summarize and explain the provisions of the proposed orders and invite public comment, and considering comments filed by interested members of the public. *See* 16 C.F.R. § 2.34(c) & (e).

[13] Prepared Statement of the FTC, *Protecting Information Security and Preventing Identity Theft*, presented by Commissioner Orson Swindle to House Comm. on Gov't Reform, Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, at 7, 14 n.24 (Sept. 22, 2004) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-information-security-and-preventing-identity/040922infosecidthefttest.pdf) ("*Comm'r Swindle's 2004 Information Security Testimony*").

[14] Pub. L. 106-102 (1999) (codified in pertinent part at 15 U.S.C. § 6804(a)(1)).

Children's Online Privacy Protection Act ("COPPA"),[15] and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[16] But these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts. For example, in COPPA, Congress authorized the Commission to sue for civil penalties in addition to the equitable monetary relief available under existing law, and authorized and directed the Commission to promulgate rules to protect children's online privacy pursuant to the streamlined procedures of the Administrative Procedure Act ("APA"), rather than using the more time-consuming procedures mandated by Section 18 of the FTC Act, 15 U.S.C. § 57a. Similarly, in both FACTA and the GLB Act, Congress directed the Commission to adopt rules addressing specified topics using streamlined APA procedures; and in FACTA, Congress also expanded the range of remedies available in Commission enforcement actions.

Finally, even if they were otherwise plausible, LabMD's arguments about the intended meaning of the past statements of the Commission or its members or staff would still be immaterial to the ultimate question of the Commission's statutory authority. "An agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone,'" and agencies "must be given ample latitude to 'adapt their rules and policies to the demands of changing circumstances." *Brown & Williamson*, 529 U.S. at 156-57 (quoting *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 863 (1984); *Smiley v. Citibank (S.D.)*, 517 U.S. 735, 742 (1996); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983); and *Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968)); *see also Verizon v. FCC*, *supra* note 5, at 19-20. Presented with the concrete circumstances of this case, the Commission concludes that it can and should address whether or not LabMD's data security procedures constitute "unfair . . . acts or practices" within the meaning of the FTC Act. To conclude otherwise would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments.

C. HIPAA and Other Statutes Do Not Shield LabMD from the Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act.

Contrary to LabMD's contention, Congress has never enacted any legislation that, expressly or by implication, forecloses the Commission from challenging data security measures that it has reason to believe are "unfair . . . acts or practices." LabMD relies on numerous "targeted statutes" that Congress has enacted in recent years "specifically delegating" to the Commission or to other agencies "statutory authority over data-security" in certain narrower fields. Motion at 15. But LabMD has not identified a single provision in any of these statutes that expressly withdraws any authority from the Commission. Thus, its argument that these more specific statutes implicitly repeal the FTC's preexisting authority is unpersuasive. "The cardinal rule is that repeals by implication are not favored. Where there are two acts upon the same subject, effect should be given to both if possible." *Posadas v. Nat'l City Bank of N.Y.*,

[15] Pub. L. 105-277 (1998) (codified in pertinent part at 15 U.S.C. §§ 6502(b), 6505(d)).

[16] Pub. L. 108-159 (2003) (codified in pertinent part at 15 U.S.C. § 1681s(a)).

296 U.S. 497, 503 (1936). Thus, one cannot conclude that Congress implicitly repealed or narrowed the scope of an existing statute (*i.e.*, Section 5) by subsequently enacting a new law unless "the intention of the legislature to repeal [is] clear and manifest; otherwise, at least as a general thing, the later act is to be construed as a continuation of, and not a substitute for, the first act . . . ." *Id.*; *see also Branch v. Smith*, 538 U.S. 254, 273 (2003) ("An implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the [later] Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'"); *Morton v. Moncari*, 417 U.S. 535, 551 (1974) ("when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective").

Nothing in HIPAA, HITECH,[17] or any of the other statutes LabMD cites reflects a "clear and manifest" intent of Congress to restrict the Commission's authority over allegedly "unfair" data security practices such as those at issue in this case. LabMD identifies no provision that creates a "clear repugnancy" with the FTC Act, nor any requirement in HIPAA or HITECH that is "clearly incompatible" with LabMD's obligations under Section 5. *See* Motion at 13. To the contrary, the patient-information protection requirements of HIPAA are largely consistent with the data security duties that the Commission has enforced pursuant to the FTC Act. Indeed, the FTC and the Department of Health and Human Services ("HHS") have worked together "to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act." HHS, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules*, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013). And the two agencies have obtained favorable results by jointly investigating the data security practices of companies that may have violated each of these statutes.[18]

LabMD further argues that HIPAA's comprehensive framework governing "patient-information data-security practices" by HIPAA-regulated entities somehow trumps the

---

[17] *See* Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 (1996) (codified in pertinent part at 42 U.S.C. §§ 1320d *et seq.*); American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, Div. A, Title XIII, and Div. B, Title IV ("Health Information Technology for Economic and Clinical Health Act") ("HITECH") (codified at 42 U.S.C. §§ 1320d-5 *et seq.*).

[18] For example, in 2009, CVS Caremark simultaneously settled HHS charges of HIPAA violations and FTC charges of FTC Act violations, stemming from the two agencies' coordinated investigations of the company's failure to securely dispose of documents containing consumers' sensitive financial and medical information. *See* FTC Press Release: *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009) (http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial); *CVS Caremark Corp.*, Consent Order, FTC Docket No. C-4259, 2009 WL 1892185 (June 18, 2009). *See also* HHS Press Release: *CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case* (Feb. 18, 2009) (http://www.hhs.gov/news/press/2009pres/02/20090218a.html). Similarly, in 2010, Rite Aid entered consent decrees to settle both FTC charges of FTC Act violations and HHS charges of HIPAA violations, which the two agencies had jointly investigated. *See Rite Aid Corp.*, Consent Order, 150 F.T.C. 694 (2010); HHS Press Release: Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case (July 27, 2010) (http://www.hhs.gov/news/press/2010pres/07/20100727a.html).

application of the FTC Act to that category of practices. Motion at 11-12. But HIPAA evinces no congressional intent to preserve anyone's ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act, and enforcement of that Act thus fully comports with congressional intent under HIPAA. LabMD similarly contends that, by enacting HIPAA, Congress vested HHS with "exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws." *Id.* at 11. That argument is also without merit. To be sure, the Commission cannot enforce HIPAA and does not seek to do so.[19] But nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act.[20]

Indeed, the FTC Act makes clear that, when Congress wants to exempt a particular category of entities or activities from the Commission's authority, it knows how to do so explicitly – further undermining LabMD's claim to an implicit "carve-out" from the Commission's jurisdiction over HIPAA-covered entities or their "patient-information data security practices." Section 5(a)(2) specifically lists categories of businesses whose acts and practices are not subject to the Commission's authority under the FTC Act. These include banks, savings and loans, credit unions, common carriers subject to the Acts to regulate commerce, air carriers, and entities subject to certain provisions in the Packers and Stockyards Act of 1921. 15 U.S.C. § 45(a)(2). Congress could have added "HIPAA-covered entities" to that list, but it did not. Similarly, the statute identifies certain types of practices that the Commission may not address, such as commerce with foreign nations in certain circumstances. *Id.* § 45(a)(3). But it provides no carve-out for data security practices relating to patient information, to which HIPAA may apply.

LabMD relies on *Credit Suisse Securities, LLC v. Billing*, 551 U.S. 264 (2007), for the proposition that industry-specific requirements in other statutes may trump more general laws such as the FTC Act. *See* Motion at 13. *Credit Suisse* is clearly distinguishable. As LabMD concedes, there was a "possible conflict between the [securities and antitrust] laws," creating a "risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, . . . or standards of conduct." *Id.* By contrast, nothing in the

---

[19] LabMD repeatedly – but incorrectly – asserts that "the FTC agrees that LabMD has not violated HIPAA or HITECH." *See, e.g.*, Motion at 13; *see also* Reply at 4 ("a company FTC admits *complied* with HIPAA/HITECH in all respects") (emphasis in original); *id.* at 5 ("FTC admits LabMD has always complied with all applicable data-security regulations"); *id.* at 12 ("FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations") (emphasis in original). The Commission does not enforce HIPAA or HITECH, and has never expressed any view on whether LabMD has, or has not, violated those statutes.

[20] Both HHS (pursuant to HIPAA and HITECH) and the FTC (pursuant to the American Recovery and Reinvestment Act of 2009) have promulgated regulations establishing largely congruent requirements concerning notification of data breaches involving consumers' private health information, but they are applicable to two different categories of firms. *Compare* 16 C.F.R. Part 318 (FTC rule) *with* 45 C.F.R. Part 164, Subparts D & E (HHS rule). LabMD correctly notes that this FTC rule does not apply to HIPAA-covered entities, *see* Motion at 12 & n.9, but the conclusion it draws from this fact is unfounded. Significantly, the Complaint in the present proceeding alleges only statutory violations; it does not allege violations of the FTC's Health Breach Notification Rule.

FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa. It is not unusual for a party's conduct to be governed by more than one statute at the same time, as "we live in 'an age of overlapping and concurrent regulatory jurisdiction[.]'" *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.C. Cir. 2001) (quoting *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1996)). LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other. Indeed, courts have consistently ruled that "the FTC may proceed against unfair practices even if those practices [also] violate some other statute that the FTC lacks authority to administer." *Accusearch*, 570 F.3d at 1194-95 (concluding that conduct may be an unlawful "unfair . . . act or practice" under the FTC Act even if it also violates the Telecommunications Act of 1996). *See also Orkin Exterminating Co.*, 849 F.2d at 1353 (rejecting proposition that a "mere breach of contract . . . is outside the ambit of [the "unfairness" prohibition in] section 5"); *Am. Fin. Servs. Ass'n*, 767 F.2d at 982-83 (FTC may ban certain creditor remedies, such as wage assignments and repossession of consumers' household goods, as "unfair . . . acts or practices" under the FTC Act, even where such conduct also ran counter to state laws against enforcing unconscionable contracts of adhesion).

Finally, LabMD argues that Congress' enactment of three new statutes addressing the Commission's authority over certain data protection matters in discrete contexts implies that Congress must have believed that, in other respects, the Commission lacked statutory authority to address data protection matters under the FTC Act. That argument, too, is without merit. First, as discussed above, in each of these statutes Congress *expanded* the enforcement and rulemaking tools that the Commission *already* possessed for addressing data security problems in discrete areas. *See supra* at 8 n.10, 9-10. LabMD identifies nothing in any of those bills or their legislative histories indicating that the Commission's authority to enforce Section 5's prohibition of "unfair . . . acts or practices" was limited in any way. Moreover, these statutes affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts.[21] Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against "unfair" practices. Congress commonly authorizes agencies to oversee entire fields while specifying, in a few areas, what minimum steps those agencies must take in exercising that authority, and the enumeration of those minimum steps does not cast doubt on the agencies' broader authority. *See, e.g.*, *Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011). And LabMD's reliance on data security-related bills that ultimately were *not* enacted into law (*see* Motion at 17-18 & n.15; Reply at 9) contradicts basic principles of statutory interpretation.[22]

---

[21] For example, in COPPA, Congress directed the Commission to promulgate rules addressing the specific duties of child-directed website operators to provide specific notices and obtain parental consent before collecting or disclosing children's personal information. *See* 15 U.S.C. § 6502(b).

[22] The fact that a proposed bill was not enacted into law does not mean that Congress consciously "rejected" it. Enacting a bill into law is a notoriously difficult and time-consuming process, given the procedural and political hurdles to be overcome before obtaining majority votes of both Houses of Congress, reconciliation of any differences between the two Houses' versions, and signature by the President. Thus, "the fact that Congress has considered, but failed to enact, several bills" typically sheds

In sum, we reject LabMD's contention that the Commission lacks authority to apply the FTC Act's prohibition of "unfair . . . acts or practices" to data security practices, in the field of patient information or in other contexts; and we decline to dismiss the Complaint on that basis.

II. THE COMMISSION HAS AUTHORITY TO ENFORCE THE STATUTE BY ADJUDICATING ALLEGED VIOLATIONS, DESPITE THE ABSENCE OF REGULATIONS, WITHOUT INFRINGING LABMD'S DUE PROCESS RIGHTS.

A. Administrative Agencies May Interpret and Enforce Statutory Requirements in Case-by-Case Adjudications, as Well as By Rulemaking.

LabMD argues that the Commission may not adjudicate whether the alleged conduct violated Section 5 of the FTC Act because the Commission "has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law." Motion at 23. LabMD asserts that "[t]he FTC's refusal to issue regulations is wrongful and makes no sense." *Id.* at 24. LabMD's position conflicts with longstanding case law confirming that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue. Thus, in the leading case of *SEC v. Chenery*, the Supreme Court recognized that the SEC had not exercised its statutory rulemaking authority with regard to the matter at issue, and squarely rejected the contention "that the failure of the Commission to anticipate this problem and to promulgate a general rule withdrew all power from that agency to perform its statutory duty in this case." 332 U.S. 194, 201-02 (1947). To the contrary: "the Commission had a statutory duty to decide the issue at hand in light of the proper standards[,] and . . . this duty remained 'regardless of whether those standards previously had been spelled out in a general rule or regulation.'" *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974) (quoting *Chenery*, 332 U.S. at 201).

The Commission has long recognized that "information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve." *See Comm'r Swindle's 2004 Information Security Testimony* at 3. Such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings, given the difficulty of drafting generally applicable regulations that fully anticipate the concerns that arise over emerging business arrangements in this rapidly changing area. As the Supreme Court has explained,

---

little, if any, light on what Congress believed or intended; and the adjudicator's "task . . . is not to construe bills that Congress has failed to enact, but to construe statutes that Congress has enacted." *Wright v. West*, 505 U.S. 277, 294 n.9 (1992) (Thomas, J.) (plurality op.); *see also Verizon v. FCC*, *supra* note 5, at 25 ("pieces of subsequent failed legislation tell us little if anything about the original meaning" of a statute, and thus such later, unenacted legislative proposals provide "an unreliable guide to legislative intent") (citations omitted).

> [P]roblems may arise . . . [that] must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective. There is thus a very definite place for the case-by-case evolution of statutory standards. And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.

Chenery, 332 U.S. at 202-03. Accordingly, "agency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *American Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). *See also FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965) ("the proscriptions [of unfair or deceptive acts and practices] in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," which "necessarily give[] the Commission an influential role in interpreting Section 5 and in *applying it to the facts of particular cases arising out of unprecedented situations*.") (emphasis added).

The Commission has enforced Section 5's prohibition of "unfair . . . acts or practices" primarily through case-by-case adjudication and litigation from the time the statute was enacted. Indeed, numerous recent cases have condemned conduct that facilitated identity theft or involved misuse of confidential consumer information as unlawful "unfair . . . acts or practices," although the practices were unprecedented and not covered by any preexisting rules. Thus, even though the Commission had never promulgated any regulations governing the creation of online checks or bank drafts without adequate verification procedures, the Ninth Circuit, in *Neovi*, easily affirmed both the district court's holding that the defendants had committed "unfair acts or practices," 604 F.3d at 1155-58, and its requirement that the defendants disgorge all revenue from the unlawful conduct. *Id.* at 1159-60. Similarly, despite the absence of any regulation prohibiting online data brokers from gathering and selling consumers' confidential information gleaned from telephone records, the Tenth Circuit affirmed a district court decision finding that the defendants' conduct constituted "unfair acts and practices" and imposing an equitable disgorgement remedy. *See generally Accusearch*, 570 F.3d 1187.

B. This Proceeding Respects LabMD's Due Process Rights

The Commission's decision to proceed through adjudication without first conducting a rulemaking also does not violate LabMD's constitutional due process rights. The courts have rejected such due process challenges to agency adjudications on numerous occasions. For example, in *Gonzalez v. Reno*, 212 F.3d 1338 (11th Cir. 2000), the court held that the agency did not violate due process in interpreting and implementing the immigration statute in an

enforcement proceeding, even though its "policy was developed in the course of an informal adjudication, rather than during formal rulemaking." 212 F.3d at 1350. *See also Taylor v. Huerta*, 723 F.3d 210, 215 (D.C. Cir. 2013) (statute enabling agency to revoke pilot's license following administrative adjudicatory proceeding "represented nothing more than an ordinary exercise of Congress' power to decide the proper division of regulatory, enforcement, and adjudicatory functions between agencies in a split-enforcement regime . . . . [Petitioner] cites no authority, and presents no persuasive rationale, to support his claim that due process requires more."); *RTC Transp., Inc. v. ICC*, 731 F.2d 1502, 1505 (11th Cir. 1984) (rejecting contention that agency's "application of its policy . . . denied them due process because the policy was announced in adjudicatory proceedings, . . . rather than being promulgated in rulemaking proceedings with notice and opportunity for comment"); *Shell Oil Co. v. FERC*, 707 F.2d 230, 235-36 (5th Cir. 1983) (noting that parties in administrative adjudicatory proceedings are not denied due process even when agencies establish new, binding standards of general application in such proceedings, so long as affected parties are given meaningful opportunities to address the factual predicates for imposing liability).

To be sure, constitutional due process concerns may arise if the government imposes criminal punishment or civil penalties for past conduct (or unduly restricts expression protected by the First Amendment) pursuant to a law that "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)). But, as the D.C. Circuit held in rejecting a constitutional due process challenge to the Commission's implementation of the Fair Credit Reporting Act,

> [E]conomic regulation is subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action. The regulated enterprise . . . may have the ability to clarify the meaning of the regulation by its own inquiry, or by resort to an administrative process. Finally, the consequences of imprecision are qualitatively less severe when laws have . . . civil rather than criminal penalties.

Trans Union Corp. v. FTC, 245 F.3d 809, 817 (D.C. Cir. 2001) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).

Here, the three-part statutory standard governing whether an act or practice is "unfair," set forth in Section 5(n), should dispel LabMD's concern about whether the statutory prohibition of "unfair . . . acts or practices" is sufficient to give fair notice of what conduct is prohibited. In enacting Section 5(n), Congress endorsed the Commission's conclusion that "the unfairness standard is the result of an evolutionary process . . . . [that] must be arrived at by . . . a gradual process of judicial inclusion and exclusion." *Policy Statement on Unfairness*, 104 F.T.C. at 1072. This is analogous to the manner in which courts in our common-law system routinely develop or refine the rules of tort or contract law when applying established precedents to new

factual situations. As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case judicial decision in the common-law tradition." *Northwest Airlines, Inc. v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981).

LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself. The imposition of such tort liability under the common law of 50 states raises the same types of "predictability" issues that LabMD raises here in connection with the imposition of liability under the standards set forth in Section 5(n) of the FTC Act. In addition, when factfinders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages. Even so, it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified. There is similarly no basis to conclude that the FTC's application of the Section 5(n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties.

III. LABMD'S ALLEGED PRACTICES ARE "IN OR AFFECTING COMMERCE" UNDER THE FTC ACT

In Section III of the Motion to Dismiss, LabMD contends that the acts and practices alleged in the Complaint do not satisfy the statutory definition of "commerce" set forth in Section 4 of the FTC Act – *i.e.*, "commerce 'among' or 'between' states." *See* Motion at 28 (citing and paraphrasing 15 U.S.C. § 44, and asserting that LabMD's principal place of business is in Georgia; the alleged acts or practices were committed in Georgia; and its servers and computer network are located in Georgia). This argument is frivolous. The Complaint plainly alleges that LabMD "tests samples from consumers located throughout the United States." Complaint, ¶ 5; *see also* ¶ 2. Indeed, LabMD concedes in its Answer to the Complaint that it "tests samples . . . which may be sent from six states outside of Georgia: Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona." Answer, ¶ 5. Thus, the complaint unquestionably alleges that LabMD's acts and practices "have been in or affecting commerce, as 'commerce' is defined in Section 4[.]" Complaint, ¶ 2.

IV. THE ALLEGATIONS IN THE COMPLAINT STATE A PLAUSIBLE CLAIM THAT LABMD ENGAGED IN "UNFAIR . . . ACTS OR PRACTICES"

We turn next to LabMD's contention that "the Complaint does not state a plausible claim for relief" on the ground that the "Complaint's allegations are nothing more than inadequate 'legal conclusions couched as factual allegations.'" Motion at 28-29 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555 (2007)).

That is incorrect. The Complaint quite clearly sets forth specific allegations concerning LabMD's conduct and other elements of the charged violation. In particular, it includes plausible

allegations that satisfy each element of the statutory standard for unfairness: that (1) the alleged conduct caused, or was likely to cause, substantial injury to consumers; (2) such injury could not reasonably have been avoided by consumers themselves; and (3) such injury was not outweighed by benefits to consumers or competition. 15 U.S.C. § 45(n). We emphasize that, for purposes of addressing LabMD's Motion to Dismiss, we presume – without deciding – that these allegations are true. But the Commission's ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding.

A. Causation or Likely Causation of Substantial Injury to Consumers

The Complaint contains sufficient allegations to satisfy the criterion that the respondent's acts or practices "cause[d], or [were] likely to cause, substantial injury to consumers." *Id.* First, the Complaint alleges that LabMD collected and stored on its computer system highly sensitive information on consumers' identities (*e.g.*, names linked with addresses, dates of birth, Social Security numbers, and other information), their medical diagnoses and health status, and their financial transactions with banks, insurance companies, and health care providers. *See* Complaint, ¶¶ 6-9, 19, 21.

Second, the Complaint contains allegations that LabMD implemented unreasonable data security measures. These measures allegedly included (*i*) "acts of commission," such as installing Limewire, a peer-to-peer file sharing application, on a billing manager's computer, *see id.*, ¶¶ 13-19, as well as (*ii*) "acts of omission," such as failing to institute any of a range of readily-available safeguards that could have helped prevent data breaches. *See id.*, ¶¶ 10(a)-(g)).

Third, the Complaint alleges that LabMD's actions and failures to act, collectively, directly caused "substantial injury" resulting from both (*i*) actual data breaches, enabling unauthorized persons to obtain sensitive consumer information, *id.*, ¶¶ 17-21, as well as (*ii*) increased risks of other potential breaches. *Id.*, ¶¶ 11-12, 22. Notably, the Complaint's allegations that LabMD's data security failures led to *actual* security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in "unfair . . . acts or practices." The Commission has long recognized that "the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." *See Comm'r Swindle's 2004 Information Security Testimony* at 4.[23] Accordingly, we will need to determine whether the "substantial injury" element is satisfied by considering not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures

[23] *See also In re SettlementOne Credit Corp.*, File No. 082 3209, Letter to Stuart K. Pratt, Consumer Data Industry Association, from Donald S. Clark, Secretary, by Direction of the Commission, at 2 (Aug. 17, 2011) (http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819lettercdia_1.pdf) (affirming, in resolving three cases concerning data security practices alleged to violate the Fair Credit Reporting Act, that it had "applied the standard that is consistent with its other data security cases – that of reasonable security. This reasonableness standard is flexible and recognizes that there is no such thing as perfect security.")

were "unreasonable" in light of the circumstances. Whether LabMD's security practices were unreasonable is a factual question that can be addressed only on the basis of evidence to be adduced in this proceeding.

Fourth, the Complaint alleges that the actual and potential data breaches it attributes to LabMD's data security practices caused or were likely to cause cognizable, "substantial injury" to consumers, including increased risks of "identity theft, medical identity theft," and "disclosure of sensitive private medical information." *See* Complaint, ¶ 12; *see also id.*, ¶¶ 11, 21-22. These allegations clearly refute LabMD's contentions that the Complaint contains "no allegations of monetary loss or other actual harm" nor "any actual, completed economic harms or threats to health or safety." Motion at 28-29. Moreover, occurrences of actual data security breaches or "actual, completed economic harms" (*id.* at 29) are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted "unfair . . . acts or practices." *Accord Policy Statement on Unfairness*, 104 F.T.C. at 949 n.12 (act or practice may cause "substantial injury" if it causes a "small harm to a large number of people" or "raises a significant *risk* of concrete harm") (emphasis added); *accord Neovi*, 604 F.3d at 1157 (quoting *Am. Fin. Servs.*, 767 F.2d at 972).

B. Avoidability

The Complaint contains plausible allegations that these harms could not reasonably be avoided by consumers. Consumers allegedly did not have any "way of independently knowing about respondent's security failures," let alone taking any action to remedy them or avoid the resulting harm. Complaint, ¶ 12.

C. Countervailing Benefits to Consumers or Competition

Finally, the Complaint alleges that the alleged conduct did not even benefit LabMD, much less anyone else (*id.*, ¶ 20), and that LabMD could have remedied the risks of data breaches "at relatively low cost" (*id.*, ¶ 11). These allegations provide a plausible basis for finding that the harms to consumers were not outweighed by other benefits to consumers or competition. Again, Complaint Counsel will need to prove these allegations, and LabMD will have the opportunity to refute them, on the basis of factual evidence presented at the upcoming hearing.

* * * * *

For the reasons discussed above, we deny LabMD's Motion to Dismiss.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice **IS DENIED.**

By the Commission, Commissioner Brill recused.

Donald S. Clark
Secretary

SEAL:
ISSUED: January 16, 2014

EXHIBIT 23

PUBLIC
PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
05 12 2014
SECRETARY
ORIGINAL

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	**DOCKET NO. 9357**
	)	
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	**ORAL ARGUMENT REQUESTED**

RESPONDENT LabMD, INC.'S REPLY IN SUPPORT OF MOTION FOR SUMMARY DECISION

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9100
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

PUBLIC

INTRODUCTION

Complaint Counsel's Opposition and supporting materials confirm that LabMD ("LabMD Inc.") is entitled to summary decision as a matter of law because the FTC lacks jurisdiction over LabMD's PHI data-security and has not provided constitutionally adequate notice of what PHI data-security practices it thinks Section 5 prohibits or requires HIPAA-covered healthcare providers like LabMD to implement.

Granting LabMD's motion is also in the interest of justice and fundamental fairness. For example, a federal District Court recently noted that since late 2012, there was "already a history of acrimony and … on behalf of the agency the exertion of authority in a mean-spirited way" against LabMD. Hearing Trans., *LabMD v. FTC*, No. 1:14-cv-810-WSD, at 47:19-21 (May 7, 2014) (the "PI Trans.") (Ex. 1). After learning that the Federal Trade Commission ("FTC") has been monitoring LabMD's CEO's website and hearing the FTC counsel's explanation, the Court said: "This is taking an interesting and troubling turn which … [the Court] never expected" due to "an admission by an FTC lawyer that they monitor blogs routinely of companies for whatever purposes…." PI Trans. 27:5-9. The Court described parts of the FTC investigation of LabMD as "a sad comment on your agency" and "strik[ing the Court] as almost being unconscionable." PI Trans. 77:9-10, 15. The Court told the FTC that "by your conduct, you have taken" a cancer-detection healthcare provider "out of the market it looks like." PI Trans. 89:2-3.

More broadly, the Court explained:

> [T]here are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.…
>
> [H]ow does any company in the United States operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that's what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did. And if you

PUBLIC

> want to conform and protect people, you ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.
>
> [I]t's hard for a company that wants to—even a company who hires people from the outside and says what do we have to do, and they say you have to do this, but I can't tell you what the FTC rules are because they have never told anybody. Again, I think the public is served by guiding people beforehand rather than beating them…after-hand.

PI Trans. 94:14-17, 94:25-95:3, 95:7-15. Thus, in consideration of the above commentary and for the reasons explained below, LabMD's Motion for Summary Decision should be granted.

ARGUMENT

As LabMD has previously argued, the FTC lacks Section 5 "unfairness" authority to regulate data-security generally, and specifically for PHI, and Section 5(n)'s text, standing alone, cannot under any circumstances provide constitutionally adequate fair notice of prohibited or required data-security practices. *See* Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Nov. 12, 2013); Reply ISO Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Dec. 2, 2013). For the reasons set forth therein, the Commission's Order Denying Respondent LabMD's Motion to Dismiss ("MTD Order" or "January 16 Order"), *In the Matter of LabMD*, Inc., FTC Dkt. 9357 (Jan. 16, 2014), correctly used the standard for motions to dismiss.

Using the standard for deciding motions for summary judgment, the Commission should grant LabMD's motion for at least two reasons.

First, as applied to LabMD specifically, this enforcement action violates due process under controlling law because LabMD never received constitutionally adequate notice of what PHI data-security practices it was required to or prohibited from implementing that are different

PUBLIC

from and in addition to those required by HIPAA, HITECH, and HHS regulations implementing those statutes.[1]

Second, Health and Human Services ("HHS") and state attorneys general have exclusive jurisdiction over healthcare providers' PHI data-security practices under HIPAA and HITECH, and the FTC's Section 5 "reasonableness" test conflicts with and layers inconsistent and additional requirements on top of those statutes. Thus Section 5 "unfairness" is plainly repugnant to these statutes and thus the FTC lacks Section 5 "unfairness" jurisdiction over HIPAA-covered entities' PHI data-security.

I. AS APPLIED TO LabMD, THE FTC'S "REASONABLENESS" STANDARD VIOLATES DUE PROCESS.

A. Due Process Requires Fair Notice of Prohibited Or Required Conduct.

Due process requires fair ex ante warning of prohibited or required conduct.[2] *Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)). A regulatory standard fails to give fair warning if it "'forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application.'" *Georgia Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005 (11th Cir. 1994) (quoting *Connally*, 269 U.S. at 391). The Supreme Court has repeatedly affirmed this principle. *See Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012); *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012).

---

[1] Courts are obligated to construe statutes to avoid constitutional problems if it is fairly possible to do so. *Boumediene v. Bush*, 553 U.S. 723, 787 (2008). The Commission should apply this principle to the Commission's January 16 Order. Under the facts of this case, due process requires granting this motion.

[2] Due process fair notice requirements apply here. *Ga. Pac. Corp. v. OSHA*, 25 F.3d 999, 1001 (11th Cir. 1994) (due-process fair-notice requirements apply to $480 administrative citation); *U.S. v. Chrysler Corp.*, 158 F.3d 1350, 1355-56 (D.C. Cir. 1998) (car recall); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002) (forfeiture); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51 (D.C. Cir. 2000) (license revocation); *Trinity Broad. v. FCC*, 211 F.3d 618, 619 (D.C. Cir. 2000) (license renewal). Complaint Counsel admits this. MSD Opp. at 10 (FTC "did not state … it is exempt from fair notice doctrine.").

PUBLIC

The FTC, "as enforcer of the Act, retains the responsibility to state with ascertainable certainty what is meant by" its putative Section 5 "unfairness" PHI data-security standards. *Georgia Pac. Corp.*, 25 F.3d at 1005; *see Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (if statute and "policy statements" are unclear and regulated entity's interpretation reasonable, that entity may not be punished). The FTC has not stated with ascertainable certainty PHI data security standards that meet its section 5 "unfairness" tests.

An FTC Commissioner with "a significant amount of experience operating with the model … [they] use at the Federal Trade Commission" candidly and accurately described the FTC's Section 5 "unfairness" data-security regime thus:

> The FTC's process is enforcement-centric rather than rulemaking-centric. As such, it is *ex post* rather than *ex ante* and case-by-case rather than one-size-fits-all. And because an enforcement action requires a complaint and a case to move ahead, the FTC's method typically focuses on actual, or at least specifically alleged, harms rather than having to predict future harms more generally.

LabMD Motion for Summary Decision, *In the Matter of LabMD*, FTC Dkt. 9357 ("MSD") at Ex. 9 pp. 10-11 (Remarks of Commissioner Ohlhausen, FTC, "The Procrustean Problem with Prescriptive Regulations,") (Mar. 18, 2014) (the "Commissioner Statement").

But it is fundamentally unfair, unjust, and unconstitutional to punish a company for allegedly doing or not doing something without first providing fair warning of prohibited or required conduct. Complex, new, and novel academic legal theory about "systemic knowledge problems" allegedly associated with normal, traditional rulemaking processes that not only are transparent and involve meaningful public participation but also provide fair ex ante notice of required or prohibited conduct does not change this. *Cf. id.* Though some may find it "Procrustean," the notion that basic due process requires fair warning of prohibited or required

PUBLIC

conduct is simple, timeless, and constitutionally required. *Connally*, 269 U.S. at 391; *SmithKline*, 132 S. Ct. at 2168; *Fox TV Stations, Inc.*, 132 S. Ct. at 2317.

At a minimum, if the FTC wishes to impose PHI data-security requirements on HIPAA-covered entities more rigorous than, inconsistent with, and different from those set by HIPAA, HITECH, and HHS regulations and objective medical-industry custom and practice, as Complaint Counsel is admittedly doing here, it must give those entities some notice that it is doing so. *S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273, 1283 (5th Cir. 1981) (discussing duty to promulgate regulations). The FTC's lack of fair notice violates LabMD's due process rights.

B. Complaint Counsel's "Guidance On Reasonable Data Security."

Complaint Counsel "disputes" LabMD's claim that the FTC has never promulgated data-security regulations, guidance, or standards under Section 5. Complaint Counsel's Public Statement of Material Facts ("CC SOF"), *In the Matter of LabMD, Inc*., FTC Dkt. 9357, at 13 (May 7, 2014). They cite three examples of what they describe as FTC "guidance on reasonable data security." *See id.* Each is addressed in turn below.

First, they cite FTC Facts for Business, Security Check: Reducing Risks to your Computer Systems (June 2003). This document was not published in the Federal Register. It correctly indicates that the FTC only has data-security enforcement authority with respect to financial institutions, which LabMD is not: "For financial institutions, it's an imperative; The Gramm-Leach-Bliley Act and the Safeguards Rule…require financial institutions to have a security plan…." CC SOF at Ex. 33. This document omits mention of HIPAA-covered healthcare providers. It does not say that failure to implement "reasonable and appropriate" PHI

PUBLIC

data security is an "unfair" trade practice banned by Section 5. In fact, Section 5 is not mentioned at all.

Next, they cite congressional testimony: Protecting Information Security and Preventing Identity Theft, Prepared Statement of the FTC before Subcomm. on Tech., Info. Policy, Intergov't Relations, and Census, Comm. On Gov't Reform, U.S. House of Representatives. (Sept. 22, 2004) (the "Swindle Testimony"). First, businesses, particularly small businesses, have no obligation to scour congressional testimony before a subcommittee for clues about what an agency most doctors are not familiar with thinks. Second, what the FTC tells Congress cannot establish binding duties and obligations. Third, this testimony provides no meaningful guidance or notice.

Orson Swindle's discussion of "reasonable security procedures" is limited to the Gramm-Leach-Bliley Safeguards Rule, which only applies to financial institutions, and even then just outlines what he calls "principles." CC SOF at Ex. 34 pp 3-4. Swindle does mention Section 5 of the FTC Act but says: "To date, the Commission's security cases have been based on its authority to prevent deceptive practices." CC SOF at Ex 34 p. 7. In footnote 24, he elaborates, mentioning in passing Section 5 "unfairness" and "deception" authority and explaining that "[t]he Commission has used this authority in appropriate case to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'" CC SOF at Ex 34 p. 14 n.24.

Swindle's subcommittee testimony is irrelevant and is not notice of anything at all. LabMD has not been accused of a "deceptive" trade practice like Internet "phishing." Businesses cannot be expected to go rooting around in footnotes of congressional subcommittee testimony to attempt to divine compliance obligations.

PUBLIC

Finally, Complaint Counsel cites a FTC consent order as "guidance," *In re The TJX Cos.*, FTC Dkt. No. C-4227 (July 29, 2008), even though, as explained below, Section 5 specifically bars the FTC from seeking to enforce these against third parties. Another problem with this putative Section 5 "unfairness" data-security "guidance" is that Complaint Counsel admits that the alleged P2P "security incident" occurred *after* this consent order was issued, and that LabMD removed Limewire from the billing computer *before* then in May 2008. *See* Complaint Counsel's Pre-Trial Br. ("CC Pretrial Br."), *In the Matter of LabMD*, Inc., FTC Dkt. 9357, at 46-47 (May 2, 2014). A third problem is that it pre-dates the first consent order involving an entity partially covered by HIPAA and a joint, parallel HHS enforcement action in the context of dumpster diving. HHS, "CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case," http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html (noting that *In re CVS Caremark Corp.* consent order (June 18, 2009) "is the first instance in which OCR has coordinated investigation and resolution of a matter with the FTC").

More fundamentally, this consent order says nothing about what the respondent allegedly did wrong, *i.e.*, why the FTC thought its alleged data-security practices constituted "unfair" trade practices banned by Section 5. The consent order says nothing about the underlying facts, does not mention what TJX's business is, and does not mention in even general terms what data-security practices TJX allegedly implemented or did not implement. It only notes that "The TJX Companies, Inc." is a Delaware corporation. CC SOF at Ex. 35 p. 2. It does not even outline with any specificity what TJX is required to do or why it is required to do it.

Tellingly, however, the *twenty-nine* pages of Complaint Counsel's Pretrial Brief in which they argue that "LabMD Failed to Provide Reasonable and Appropriate Security for Personal

PUBLIC

Information on its Computer Networks" solely cites the spring 2014 Hill paid litigation expert reports (dozens of times) and does not mention any of this alleged FTC "guidance." *See* CC Pretrial Br. at 22-51; PI Trans. 68:20-25 ("Q. … [D]oes Dr. Hill rely on any published materials from FTC? A. She doesn't, which I found interesting. I would have thought that … the expert witness for the FTC would have been referencing FTC guidance for security requirements. She did not….").

There is no genuine dispute as to this material fact.

C. Section 5 and APA Statutory Bar On Use of Consent Orders and Other Internet Postings as "Guidance."

i. APA Federal Register Publication Requirement.

The APA statutorily bars Complaint Counsel from enforcing requirements it claims are set forth in the above-described materials except insofar as these materials are duly published in the Federal Register. 5 U.S.C. § 552(a). Specifically, the APA obligates the FTC to "separately state and currently publish in the Federal Register for the guidance of the public … *statements of general policy or interpretations of general applicability* formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D)(emphasis added). The APA statutorily bars agencies like the FTC from enforcing against companies like LabMD statements of general policy and interpretations of general applicability "[e]xcept to the extent that a person has actual and timely notice of the terms thereof…." 5 U.S.C. § 552(a); *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001) (Internet notice is not an acceptable substitute for publication in the Federal Register). There is no allegation that LabMD had actual notice of any of this.

Compliance Counsel's suggestion that LabMD had any duty to comply with or even to consult for "guidance" any of these materials should be rejected. *See also Gen. Elec. Co. v.*

PUBLIC

EPA, 290 F.3d 377, 382-83 (D.C. Cir. 2002) (holding that agency guidance document that imposes binding duties and obligations violates the APA).

Even the FTC's own Operating Manual belies Complaint Counsel's claim that the FTC has provided Section 5 data-security "guidance," as the chapter on "Industry Guidance" says nothing about use of consent orders, congressional testimony, and assorted Internet postings. *See* FTC Operating Manual, Ch. 8, *available at* http://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch08industryguidance.pdf (accessed May 8, 2014). Instead, it recognizes that "[t]he Administrative Procedure Act requires … that interpretative rules and policy statements be published in their final form in the Federal Register." *Id.* at 5, §.3.6.4.

ii. Section 5's Statutory Bar on Use of Consent Orders as "Guidance."

Section 5 also statutorily bars Complaint Counsel from attempting to enforce alleged "standards" set forth in the FTC's putative "common law" of consent orders. Congress *specifically barred* the Commission from enforcing a "consent order" against anyone who is not a party to it. 15 U.S.C. § 45(m)(1)(B); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir. 2007) ("[T]he FTC Act … with regard to consent orders … specifically provides that the Commission cannot enforce them against non-parties."). Agencies cannot regulate by consent orders, *see Gen. Elec. Co.*, 290 F.3d at 382-83, which "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement," *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). Moreover, consent orders do not bind the Commission and restrict its discretion in future actions and thus cannot provide fair notice. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999).

PUBLIC

The Commission's January 16 Order also rejected Complaint Counsel's claim that consent orders create a "common law" of data-security that LabMD should have followed. *See* MTD Order at 15-16.

D. Complaint Counsel's Application of "Reasonableness" Violates Due Process.

As noted above, Complaint Counsel's Opposition, Statement of Facts, and Pretrial Brief confirm that PHI data-security standards set by HIPAA, HITECH, and HHS regulations implementing those statutes (and LabMD's compliance or noncompliance with those standards) are "irrelevant" to their case-in-chief and that they are holding LabMD to "standards" sprung on LabMD for the first time in spring 2014 in their paid litigation "expert's" reports. They thereby confirm that summary decision in LabMD's favor is constitutionally required. *See* CC Pretrial Br. 22-51; PI Trans. 58:10-69:14.

Under controlling law, because Section 5(n) is too general, standing alone, to provide fair notice, as the Commission acknowledges by layering upon it a "reasonableness" test, *see* MTD Order at 18-19, "due process requires" that the Commission's Order's "reasonableness" standard be read to incorporate an "objective industry practice standard."[3] *S&H Riggers*, 659 F.2d at 1285; *Fla. Mach. & Foundry, Inc. v. OSHRC*, 693 F.2d 119 (11th Cir. 1982) (industry-specific standards control).

Complaint Counsel wrongly claims that HIPAA/HITECH compliance is, at best, an "affirmative defense." CC SOF at 6, 10-12. But binding precedent holds that Complaint Counsel "bears the burden of proving that" LabMD failed to adopt PHI data-security practices

---

[3] The sole exception requires proof of "clear actual knowledge" of problems and failure to act. *Fla. Mach. & Foundry, Inc.*, 693 F.2d at 120; *S&H Riggers*, 659 F.2d at 1285. Complaint Counsel has never alleged (and no evidence supports) that. In fact, the Complaint alleges the contrary—when LabMD learned of Limewire, it promptly took remedial steps, including but not limited to removing it. *See* Compl.¶ 20 (LabMD "removed … [Limewire] from the billing computer in May 2008, after receiving notice.").

PUBLIC

that were customary in the medical industry at the time of the alleged violations. *S&H Riggers*, 659 F.2d at 1285; *Fla. Mach. & Foundry*, 693 F.2d at 120 ("[A] standard of this generality requires only those protective measures which the *employers' industry* would deem appropriate…." (emphasis added)); *see B&B Insulation*, 583 F.2d at 1370 (industry-specific standard, e.g., what is customary for sausage industry or roofing industry).

Complaint Counsel thus has the affirmative burden of proving that LabMD's PHI data-security practices were inconsistent with and less protective of PHI than the objective medical-industry practice standard for PHI data-security practices that were customary for businesses of LabMD's size and nature to adopt at the time that such LabMD practices were used. For example, Complaint Counsel must prove that LabMD's PHI data-security practices in 2005 fell below those that were customary in 2005 for a *healthcare provider* (not IT company) of LabMD's size and nature in 2005 in the medical industry to use—as opposed to IT industry best practices in 2014. HIPAA, HITECH, and HHS PHI data-security regulations reflect the objective medical-industry practice standard for data-security.

When Complaint Counsel says that HIPAA, HITECH, and HHS regulations are "irrelevant," they admit they cannot prove this and have no intention of attempting to do so. Complaint Counsel has offered no evidence as to what medical-industry PHI data-security practices are or were at any specific point in time for healthcare providers of LabMD's size and nature during the relevant time period. They have not accused LabMD of violating medical-industry PHI data-security statutes and regulations that apply to LabMD. Therefore, Complaint

PUBLIC

Counsel cannot even establish the constitutionally mandated objective medical-industry practice standard of care, let alone prove that LabMD's conduct fell below it.[4]

Thus, the Commission's January 16 Order's "reasonableness test, as applied to LabMD by Complaint Counsel, violates due process. Under controlling precedent, Complaint Counsel's case is constitutionally defective as a matter of law.

II. THE FTC LACKS SECTION 5 "UNFAIRNESS" JURISDICTION OVER HIPAA-COVERED ENTITIES.

Complaint Counsel argues that whether their after-the-fact paid-litigation-expert "reasonableness" standard is plainly repugnant to and irreconcilably conflicts with PHI data-security *standards* for HIPAA-covered healthcare providers like LabMD—set by Congress and HHS through duly-enacted legislation and normal notice-and-comment rulemaking (specifically, HIPAA, HITECH, and HHS regulations implementing those statues) in a transparent manner with meaningful public participation—"should be addressed at trial…." Complaint Counsel's Resp. in Opp. to Respondent's Mot. for Summary Decision ("CC Opp."), *In the Matter of LabMD, Inc*., Dkt. No. 9357, at 12 (May 5, 2014).

But there is no factual dispute about PHI data-security standards set by HHS regulations (unlike "unfairness reasonableness," regulations specify standards).[5] Complaint Counsel admits

---

[4] There can be no genuine disputes about her "reasonableness" opinions because her reports must "contain a complete statement of all opinions to be expressed and the basis and reasons therefore…." 16 C.F.R. § 3.31A(c).

[5] *See* 42 U.S.C. § 1320d-2(d)(1) (establishing "Security standards for health information" and providing HHS with enforcement authority); 65 Fed. Reg. 82,462 (Dec. 28, 2000) (HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334 (Feb. 20, 2003) (HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566 (Jan. 25, 2013) (HHS's HITECH Rule). LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, *In the Matter of LabMD*, Inc., FTC Dkt. No. 9357, at 22 n. 15 (Nov. 22, 2013) ("HHS published guidance to entities subject to HIPAA, such as LabMD …."); Compl. ¶¶ 3-4, 6, 9; see 42 U.S.C. §1320d(3)-(4) (defining terms); 45 C.F.R. § 160.103 (same).

PUBLIC

that HIPAA, HITECH, and HHS regulations are "irrelevant" to their case-in-chief.[6] CC SOF at 6, 10-12; CC Opp. at 4-5; *see* CC Pre-Trial Br. at iv-vii, 1-72 (not citing or mentioning HIPAA, HITECH, or HHS regulations); LabMD MSD at 6. Their Pretrial Brief shows they solely rely on Hill's reports for "standards." CC Pretrial Br. 22-51 (solely citing Hill dozens of times). Their expert, Hill, does not apply HIPAA, HITECH, or HHS regulations to LabMD's PHI data-security, and her "standards" are different from, inconsistent with, and more rigorous than PHI data-security standards set by applicable statutes and regulations. *See* LabMD MSD at 19-22 & Ex. 12; PI Trans. 58:10-69:13. HHS (and state attorneys general) has exclusive jurisdiction under HIPAA and HITECH. The FTC enforces neither. MTD Order at 12 & n.19.

Section 5 was last amended in 1994; HIPAA was enacted in 1996. *See* MTD Order at 4-5, 11 n.17. Assuming the Section 5 "unfairness" otherwise extended to data-security, application of the *Credit Suisse* factors shows a "plain repugnancy" between the FTC's Section 5 "unfairness" data-security regime and HHS's enforcement of HIPAA/HITECH. *Credit Suisse Securities v. Billings*, 551 U.S. 265, 272, 275-76 (2007); MSD at 19-22; *see also* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, *307 n.15 (1984)("Of course, if matters involving health and safety are within the primary jurisdiction of some other agency, Commission action might not be appropriate.").

HIPAA (1996), HHS's HIPAA Privacy Rule (2000), and HHS's HIPAA Security Rule (2003) all predate the FTC's "expansion" of Section 5 "unfairness" to data-security, as Swindle admitted that as of September 22, 2004, no "unfairness" cases had been brought. Swindle Testimony at 7; *cf.* MTD Order at 8 (dating "origin" to "late 1990s" but only citing post-2006

[6] "[T]he Commission cannot enforce HIPAA and does not seek to do so…. The Commission does not enforce HIPAA or HITECH…." MTD Order at 12 & n.19.

documents). Since HIPAA was enacted in 1996, Congress could (and would) not have thought it necessary to explicitly state the FTC has no authority.[7] *Cf.* MTD Order at 12. Even if Section 5 "unfairness" otherwise conferred data-security jurisdiction, the FTC may not impose PHI data-security standards over and above HIPAA. *FTC v. A. P. W. Paper Co.*, 328 U.S. 193, 198-204 (1946).

CONCLUSION

For these reasons, LabMD's Motion should be GRANTED.

Respectfully submitted,

_____

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141

/s/ Michael D. Pepson
Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

[7] The recent vintage of the FTC's claimed Section 5 "unfairness" data-security authority is precisely why the HIPAA Privacy Rule's Implied Repeal Analysis omits mention of Section 5 but specifically discusses the FTC's data-security authority under a different, targeted statute. 65 Fed. Reg. at 82,481-82,485. HIPAA was necessary, in part, *because* the FTC has never had Section 5 "unfairness" authority over PHI. *Cf. id.* at 82,464 (HHS's HIPAA rule "establishes, for the first time, a set of…fair information practices").

CERTIFICATE OF SERVICE

I hereby certify that on May 12, 2014, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I caused to be hand-delivered twelve paper copies of the foregoing document to the following address: Document Processing Section, RFO Receiving Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610, Washington, D.C. 20024.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: May 12, 2014 By:/s/ Michael D. Pepson

2962021v2

EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, INC.	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE
	)	NO. 1:14-CV-810-WSD
v.	)	
	)	ATLANTA, GEORGIA
FEDERAL TRADE COMMISSION	)	
	)	
Defendant.	)	
	)	

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE WILLIAM S. DUFFEY, JR.,
UNITED STATES DISTRICT JUDGE

Wednesday, May 7, 2014

APPEARANCES OF COUNSEL:

For the Plaintiff: KILPATRICK TOWNSEND & STOCKTON LLP
(By: Ronald L. Raider
William D. Meyer)
Burleigh Lavisky Singleton)

DINSMORE & SHOHL LLP
(By: Reed D. Rubinstein)

For the Defendant: U.S. DEPARTMENT OF JUSTICE
(By: Lauren Fascett
Perham Gorji
Joel Marcus)

Proceedings recorded by mechanical stenography and computer-aided transcript produced by
NICHOLAS A. MARRONE, RMR, CRR
1714 U. S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
(404) 215-1486

And I believe he is still effectively expressing his speech, and, therefore, there is a legitimate reason.

THE COURT: Are you telling me as an officer of the court that after a critical blog post, that somebody at the FTC, in order to make sure that he was -- that he was not impeded in his First Amendment rights, decided the next day to 75 times make sure that the same post was up there and, therefore, it could come in and make an argument like you have just made, that the purpose of that access was to make sure that he was unimpeded in the exercise of his First Amendment rights?

MR. GORJI: Your Honor --

THE COURT: Is that what you are saying?

MR. GORJI: Your Honor, that is not the sole explanation.

THE COURT: Is that what -- is that one of your explanations?

MR. GORJI: I believe that is a legitimate reason for --

THE COURT: And is that why the -- is that why you are representing to me that the FTC accessed his blog, was to make sure that his First Amendment rights were not being impeded?

MR. GORJI: No, I'm not making that representation, Your Honor, that that is the sole reason.

THE COURT: So you are backing from what you just told me?

MR. GORJI: No, no, Your Honor. I believe that one legitimate basis for --

THE COURT: Was that a legitimate basis on behalf of your client, the FTC, the reason why they accessed the blog post 75 times the day after the post was made?

MR. GORJI: Your Honor, I would have to get FTC to provide an explanation as to why they accessed it. I can --

THE COURT: You just told me twice that's one of the reasons they accessed it. Is that one of the reasons why they accessed it?

MR. GORJI: Well, Your Honor, I know that's one of the reasons why I accessed it, for example, during the course of this litigation.

THE COURT: Did you access it on September 17th or September 18th?

MR. GORJI: No, Your Honor.

THE COURT: How many times have you accessed it?

MR. GORJI: Maybe a handful, Your Honor. But -- and that was my motivation.

But I can also surmise, Your Honor, that a government agency might think that there is possibility of statements related to the conduct -- to the conduct that FTC is trying to regulate on his postings and looking for that

reason.

Now, whether or not that is the actual motivation here, Your Honor, I can't attest to that. I can ask FTC to provide you with their explanation.

THE COURT: This is taking an interesting and troubling turn which I never expected, for an admission by an FTC lawyer that they monitor blogs routinely of companies for whatever purposes, and you don't even know the purposes except for this purpose, that the only purpose that you have expressed, which I find incredible, is that you stated on behalf of your agency that the day after this blog posting was made, that the 75 times -- assuming that's true, but even if it was seven times, that they monitored it to make sure that his First Amendment rights were not being impeded, is incredible.

MR. GORJI: Your Honor, that's not my sole explanation. My other explanation --

THE COURT: But it's one of your explanations, isn't it?

MR. GORJI: Your Honor --

THE COURT: Isn't it?

MR. GORJI: Your Honor, I think perhaps that is probably an explanation as to why I personally did it. With respect to the FTC, I don't know whether or not that motivated --

THE COURT: Was my question unclear about the accessing of the website the day after the posting? Did you not understand that?

MR. GORJI: Your Honor, your question was not unclear. I perhaps was confused, but not because of the lack of clarity of your question. I apologize to the Court.

Again, I can have the FTC provide an explanation as to why they are monitoring, and my explanation is again what I surmise, but it may not be sufficient here. And, Your Honor, if Your Honor would like, we could have FTC provide an explanation to the Court.

THE COURT: Well, let's have this rule between you and me at least. This is a hearing. I am a judicial officer, and you are an officer of the court. When I ask you a question, don't duck and cover the question. Answer the question so that I know that what you are telling me is accurate and I can rely upon it. Is that fair?

MR. GORJI: That's fair, Your Honor. I didn't intend to give the impression that I knew what the reason was. I was providing an explanation as to why I think it might be reasonable.

THE COURT: Well, that's not what you said, and the record will be clear that in answer to my two questions, that is not what you said.

MR. GORJI: Your Honor, the jurisdictional arguments are the primary arguments we do make. We do also make the 12 (b) (6) arguments, Your Honor, that do not deny your authority but that we believe the causes of action fail to state a claim.

But I would just like to put something in perspective on behalf of the government here, Your Honor, which is the history of acrimony that you perceive, this is a case that I was just very recently assigned to along with co-counsel here. Counsel who was on this case is no longer with the Department of Justice.

And so I just became aware of this transcript last week, Your Honor. And so there certainly wasn't any --

THE COURT: That's not the defendant's or my fault or my problem. That's your problem. If you want to switch lawyers, you switch lawyers.

And if you are talking about the fellow who was here on the CID, I could tell you as a result of that hearing that there was already a history of acrimony and I think on behalf of the agency the exertion of authority in a mean-spirited way.

MR. GORJI: Well, Your Honor, I can just say that --

THE COURT: And you might -- you know, I'm not saying that -- if you are just new to this case, which

MR. GORJI: Documents, papers.

THE COURT: All right. So -- and where did the police department claim that the papers -- how were the papers obtained?

By papers, you mean paper documents, that somehow they got hold of some paper documents with some patient information on it? Is that what the allegation is?

MR. GORJI: Yes, Your Honor. My understanding is they were in possession of the individuals who pled no contest to the state charges of identity theft.

THE COURT: Well, if they pled no contest, they probably cooperated. Did they tell you where they got the papers?

MR. GORJI: Your Honor, if I might inquire?

Your Honor, I don't have information as to how the documents and the information was obtained by the identity thieves.

THE COURT: Well, has anybody from the FTC gone out and interviewed the people who pled *nolo* to that to find out where it came from, to see whether or not there was indeed a security breach?

Let me tell you something, these are the most simple questions of this investigation. That you are claiming that some police department prosecuted some people for having possession of information which you are now

claiming wrongfully was not protected by LabMD, and you can't even tell me whether or not you have interviewed the people who had the data to find out where they got it to see whether or not there was a security breach or not? And yet you have implemented and instituted this investigation?

And this is your case. You are new -- I know you might be new on it, but for heaven's sakes, you are arguing to me that there is a hearing on May 20th and you don't even know.

MS. FASCETT: Your Honor, if I may just explain, just for clarity, not as an excuse. The FTC attorneys that are handling the administrative proceeding in that hearing, they I'm assuming definitely know these details. They are not present. They are not here today.

We are just -- we were just brought in from DOJ to represent this complaint in this action. So that's part of why we don't have these facts. But we represent the FTC here and we can get these facts for you.

MR. RUBINSTEIN: Your Honor, if I could?

THE COURT: I'm not --

MR. RUBINSTEIN: I --

THE COURT: Sit down.

MR. GORJI: Your Honor, my --

THE COURT: So where are those lawyers? Are they too busy to come to Atlanta today?

MS. FASCETT: Well --

THE COURT: Is that one of them sitting back there in the gallery?

MS. FASCETT: No, she's a U.S. Attorney here in Atlanta, unrelated.

THE COURT: How about this other fellow back there, is he an FTC lawyer too?

MR. MARCUS: Your Honor, we have a gentleman here from the FTC.

THE COURT: Are you involved in this investigation?

MR. MARCUS: I am personally not involved in the investigation.

THE COURT: Okay. So you are off the hook.

So far I have got four lawyers here and none of them are involved in the investigation. How about --

MR. MARCUS: We do have are a lawyer who is involved in the investigation.

THE COURT: And what's your name?

MR. SCHOSHINSKI: Good morning, Your Honor. Robert Schoshinski. I'm assistant director in the Division of Privacy and Identity Protection.

THE COURT: All right. So in this case, what investigation has been made as to the source of the documents that the police department out in California found?

MR. SCHOSHINSKI: Your Honor, the complaint counsel, so that is the FTC counsel who is litigating the complaint in the administrative action, noticed the depositions of the two individuals who pled no contest to identity theft.

One they could not serve because she was just simply not findable. The other one was in jail. We --

THE COURT: Did you try to find her?

MR. SCHOSHINSKI: Yes, we did, Your Honor. We hired several process servers. They made many attempts to try to find her but were unable to serve her.

THE COURT: And when did you first try to serve her?

MR. SCHOSHINSKI: Your Honor, I don't have the exact dates, but --

THE COURT: Well, give me an approximation.

MR. SCHOSHINSKI: Your Honor, I would say late 2013, early 2014.

THE COURT: So really late in the game, you finally decided that it made sense to go and find out with respect to one of the allegations that's the basis of your investigation that's been ongoing for months, because the CID was something I dealt with some months ago, that you finally decided -- or not you, but your lawyers finally decided that maybe it would be good to try to find the people who actually had the

information to determine where they got it?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Does that strike you as odd?

MR. SCHOSHINSKI: Your Honor, it doesn't strike me as odd. It's what --

THE COURT: Does it strike you as late?

MR. SCHOSHINSKI: Your Honor, it strikes me as the normal course of the investigation.

THE COURT: Boy, that's a sad comment on your agency, that you would wait until months before a hearing and months after you instituted an investigation on a principal claim that you are asserting, that you have not even taken any effort to interview the people that you claim had the documents that underlie the charge of a security breach. That strikes me as almost being unconscionable.

And how much money -- how much activity was there before you served those subpoenas trying to get the information from LabMD with respect to a security breach that you don't even know how it occurred? How much activity?

MR. SCHOSHINSKI: Your Honor, how would you like me to estimate?

THE COURT: Let's start in months.

MR. SCHOSHINSKI: Well, Your Honor, I believe the investigation began in January of 2010.

THE COURT: Okay. So three years before you tried

to subpoena them?

MR. SCHOSHINSKI: Your Honor --

THE COURT: I'm sorry, two and a half years.

MR. SCHOSHINSKI: Your Honor, the knowledge of this incident didn't occur until after the CID enforcement hearing up here in Atlanta. That's when we were notified that this incident had occurred, in October of 2012.

THE COURT: So you found out about the -- the incident you are talking about is the California police incident?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: All right. And how soon after you found out about the incident did you try to contact the police authorities in California to find out what they knew about the source of the information?

MR. SCHOSHINSKI: Immediately.

THE COURT: And what did they tell you?

MR. SCHOSHINSKI: They told us that they did not know.

THE COURT: And then what did you do next, and how soon did you do it?

MR. SCHOSHINSKI: We shared the information with LabMD concerning the -- what we found out once we were able to confirm that it was LabMD's information, and we then attempted to find out further from the California police

department what they knew about the source of this information.

THE COURT: And what did they tell you they knew about the source?

MR. SCHOSHINSKI: They told us they were not able to get the source from the defendants in the case.

THE COURT: Did you talk to the prosecutor of the case as well?

MR. SCHOSHINSKI: I don't believe so, Your Honor.

THE COURT: And so you tried to track down one of the two defendants. Did you try to track down the second of the two defendants?

MR. SCHOSHINSKI: Yes, Your Honor. We actually obtained service on the second defendant, who was in jail. We noticed his deposition in the action, went to take his deposition, and he pleaded the Fifth Amendment and refused to answer questions.

THE COURT: So sitting here today, you have no idea where the documents came from, whether they came from LabMD or some other source? Is that a fair thing to say?

MR. SCHOSHINSKI: No. We believe they were LabMD's documents.

THE COURT: Well, they might have been LabMD's documents, but you don't know how they got into the possession of the two individuals that you tried to contact

that pled guilty to this offense?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: So you have no information to establish how those documents were obtained; is that right?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And you are still proceeding on this claim?

MR. SCHOSHINSKI: Yes, Your Honor, because the claim is not concerning that incident alone. It's concerning --

THE COURT: All right. But are you still proceeding on that claim?

MR. SCHOSHINSKI: We are proceeding on that evidence, Your Honor.

THE COURT: And that evidence relates to other claims, because you have other documents that were found in other places?

MR. SCHOSHINSKI: That evidence relates to the potential injury suffered by consumers as a result of exposure of this information.

THE COURT: Are you serious about that last response?

MR. SCHOSHINSKI: Yes, Your Honor, I am.

THE COURT: So you don't know where the documents came from, you don't know how these people got the possession

of it, you don't know whether they originated from LabMD or some other place, but you are going to use that to show that, because they committed identity theft, that certain individuals were damaged by documents, the source of which you don't even know?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Holy cow.

So what's the other incident that you are relying on?

MR. SCHOSHINSKI: The other incident is the exposure of the insurance agent file of several thousand consumers.

THE COURT: And when was that?

MR. SCHOSHINSKI: That was in 2008, Your Honor.

THE COURT: And that was through the file-sharing program?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And how do you know that they came through the file-sharing program?

MR. SCHOSHINSKI: We know because third parties found the file on file-sharing programs.

THE COURT: Well, I accept that. How do you know that they came through the file-sharing program that was loaded on a computer at LabMD?

MR. SCHOSHINSKI: Based on the evidence we obtained

than it is in this case, and then they are arguing that, although I'm co-equal to the judge in New Jersey, that because it came to me a different way, that I can't.

I suspect that they would love to travel forward on the New Jersey decision because it favors them and that they will try to deny the opportunity for another judge to weigh in.

But I think it's a significant -- you ought to find a way, unless you are so hell bent on expanding this jurisdiction or advocating this jurisdiction, to find some way to decide this legal issue.

And I understand why you are doing what you are doing. I have been alive long enough to understand how government and their agencies work. I have been a member of an agency and I understand its impact on defendants or in this case on parties that are under investigation. I understand that too because I have done that as well.

But I think that there is a fundamental jurisdictional legal issue, and there ought to be some way of getting a more definitive ruling than what you have right now.

Because I would hope that you would think that in this current healthcare environment, that the more competition and providers there are for medical detection devices or processes like those offered by LabMD, that the

better off the consuming public is and the better off patients will be. But by your conduct, you have taken one out of the market it looks like.

And if I was an agency head, I would say there has got to be some way of being satisfied that this doesn't happen again, however it happened, and to make sure that we have as many providers as possible out there determining whether or not people do or do not have cancer.

And that that would mean a good faith, transparent, authentic discussion about what your concerns are, and trying to get those allayed by some process which would not be a twenty-year monitoring.

You know, I have defended people that had twenty-year monitoring responsibilities by an agency, big companies, and it's very, very expensive, and it's really intrusive, and in my personal opinion, having been on both sides, they generally are not necessary.

But there is never a middle ground. There should be.

But I would think that it would be in the benefit of all the parties here to say whatever happened, it can't happen again, but whatever you are doing ought to continue to be done, because it benefits the consuming public, which I think is who you are supposed to be protecting under reasonable certainties, that the consuming public would be

Congress, and we turn things down.

I think good lawyers -- and he was an agency lawyer for a long time and ran the Southern District for a long time as United States Attorney -- that that lesson has always stuck with me.

So where we are now is I have given you my insights about this. I understand there is no more evidence to be presented.

I don't need any more -- I guess you can cross-examine him if you want. All I hear him saying is that he doesn't like your expert's report and he would have done something differently and he's claimed that HIPAA is what should be, because there are specific standards there -- I think that you will admit that there are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.

I too find how does any company in the United States operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that's what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did.

And if you want to conform and protect people, you

ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.

But I think that's what happens when you jump too quickly into something that you want to do, and whether that's circumstances or whether that's agency motivation, I don't know. But it seems to me that it's hard for a company that wants to -- even a company who hires people from the outside and says what do we have to do, and they say you have to do this, but I can't tell you what the FTC rules are because they have never told anybody.

Again, I think the public is served by guiding people beforehand rather than beating them after they -- after-hand. But the assistant director doesn't have the authority to do that. He reports to the deputy director, who reports to the director, who reports to the commission. So he's way down in the pecking order.

So I understand what this witness said.

I suspect that this witness will say that he never consulted with LabMD before about their security processes. He's just come in to opine on the opinions offered by Ms. Hill. Is that correct?

THE WITNESS: Correct.

THE COURT: I kind of wish he had been there before.

EXHIBIT 24

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
	)	**PUBLIC**
LabMD, Inc.,	)	
a corporation.	)	

RESPONDENT LabMD, INC.'S REPLY TO COMPLAINT COUNSEL'S RESPONSE IN OPPOSITION TO RESPONDENT'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and Counsel to Cause of Action.

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

PUBLIC

INTRODUCTION

FTC's Opposition to LabMD's Motion is remarkable in only two respects. First, it demonstrates FTC has discarded rule-of-law and constitutional values for boundless bureaucratic power and discretion. Second, it shows FTC will distort the law and even re-write history to justify its power-grab.

FTC's Opposition's admissions and arguments demonstrate only that FTC lacks Section 5 authority over patient-information data-security, and that its standardless, blame-the-victim *ex post* enforcement tactics violate due process and fail to provide LabMD with constitutionally-adequate fair warning of the data-security standards FTC believes Section 5 forbids or requires.

STANDARD OF REVIEW

FTC does not respond to many arguments made in LabMD's Motion to Dismiss (Mot.). "[F]ailure to respond to an argument…acts as a concession" and thus an admission. *CREW v. Cheney*, 593 F. Supp. 2d 194, 229 (D.D.C. 2009).

FTC admits it must prove Congress intended to delegate it specific authority to regulate patient-information data-security. *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). FTC also admits the FRCP 12(b)(6) standard controls here under *In re S.C. State. Bd. of Dentistry*, 138 F.T.C. 229, 232 (F.T.C. 2004). *See* FTC Opp. to Mot. (Opp.) 3. Yet FTC claims without citing any controlling (or on-point) authority that the *Iqbal/Twombly* standard for 12(b)(6) motions does not apply. Opp. 25. Because FRCP 12(b)(6) applies here, as FTC admits, *Iqbal*/*Twombly* apply as well. *See Jones v. Horne*, 634 F.3d 588, 595-96 & n.4 (D.C. Cir. 2011)(*Iqbal/Twombly* sets standard for 12(b)(6) motions).

PUBLIC

ARGUMENT

I. FTC LACKS SECTION 5 "UNFAIRNESS" AUTHORITY OVER DATA-SECURITY.

A. HIPAA/HITECH Control, And FTC May Not Over-File.

Citing no controlling authority or explicit statutory command, FTC wrongly claims "concurrent" jurisdiction over HIPAA/HITECH patient-information data-security.

FTC admits LabMD is and always has been a HIPAA-covered entity regulated exclusively by HHS under HIPAA/HITECH.[1] It also admits LabMD is specifically exempted from FTC's HITECH rule. *Cf.* Mot. 12 & n.9. It offers no explanation why HITECH, Pub. L. 111-5 §13424(b)(1), directs HHS and FTC to determine *which* agency is best equipped to enforce HITECH against non-HIPAA-covered entities (FTC agrees that HHS exclusively regulates HIPAA-covered entities like LabMD). It also ignores HIPAA's directive to HHS—not FTC—to "adopt [data-]security standards" for "health information." 42 U.S.C. §1320d-2(d)(1); 42 U.S.C. §1320d(4)(defining "health information").

Even if Section 5 covered data-security, HIPAA/HITECH are "precisely drawn, detailed statute[s that] pre-empt" Section 5's "more general remedies." *EC Term of Years Trust v. U.S.*, 550 U.S. 429, 433 (2007). Through HIPAA/HITECH, Congress deliberately targeted specific data-security problems with specific solutions, and these specific statutes govern over whatever "general" Section 5 authority FTC might have. *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012). Otherwise, HIPAA-covered companies like LabMD lack data-security safe-harbor and certainty, contrary to HHS's regulatory intent.

[1] FTC incorrectly claims LabMD only cites one HITECH provision to support its argument. But LabMD cites multiple HIPAA provisions. Mot. 11-13 & nn.4,9.

PUBLIC

See 78 Fed. Reg. 5,566, 5,644 (Jan. 25, 2013)(encouraging covered entities to use encryption safe-harbor); 65 Fed. Reg. 82,462, 82,543 (Dec. 28, 2000)(discussing safe-harbor).

FTC says "Congress's intent to preempt or repeal…FTC's unfairness authority" must be clear-and-manifest. Opp. 6. This distorts the law, for implied repeal may be found even "absent 'a clearly expressed congressional intention'" where, as here, two statutes irreconcilably conflict. *Carcieri v. Salazar*, 555 U.S. 379, 395 (2009).

FTC attempts to avoid *Credit Suisse v. Billing*, 551 U.S. 264 (2007), with the specious argument that the Court explicitly limited the rule there to conflicts between antitrust and securities laws. Opp. 7. But nowhere in *Billing* does it say this.[2] Instead, *Billing* fleshes out the analysis for determining a "clear repugnancy." *Billing* confirms that HIPAA/HITECH irreconcilably conflict with Section 5, and, being more recent and more specific than Section 5, control. *See Billing*, 551 U.S. at 276, 285. Even if the canon against implied repeal is applied here, Section 5 is displaced by HIPAA/HITECH. *See EC Trust*, 550 U.S. at 434-36.

FTC claims that because HITECH was enacted "*after*…[FTC] had brought a half-dozen unfairness cases relating to data security," Congress has blessed its power-grab. Opp. 7 n.4. That, too, distorts the law. Congress's failure to express any opinion is not probative of legislative intent. *Rapanos v. U.S.*, 547 U.S. 715, 749-50 (2006).

Finally, FTC's reliance on *two recent consent orders* in cases also involving allegations of Section 5 "deception" and HIPAA violations is another irrelevant distraction.[3] Here, the question is not whether Section 5 and HIPAA/HITECH authorities might be "complementary"

---

[2] *See* Jesse Markham, *The Supreme Court's New Implied Repeal Doctrine*, 45 GONZ. L. REV. 437,475 (2009)(*Billing* "not limited to…interplay between antitrust law and economic regulation.").

[3] *In re CVS Caremark* "is the first instance in which [HHS] OCR…coordinated …with…FTC." http://www.hhs.gov/news/press/2009pres/02/20090218a.html.

PUBLIC

under some circumstances. Instead, it is whether FTC's "unfairness" authority allows FTC to over-file HHS and punish a company FTC admits *complied* with HIPAA/HITECH in all respects. FTC's interpretation of Section 5 wrongly eviscerates Congress's HIPAA/HITECH enactments and HHS's regulatory scheme.

B. FTC Lacks "Unfairness" Authority Over Data-Security.

FTC says its position that "companies *should* engage in 'reasonable' [data-security] practices…is premised on Congress's mandate" in 15 U.S.C. §45(n). Opp. 2 (emphasis added). This claim, yet again, distorts the law. Congress's subsection (n) mandate was to rein in FTC's abuse of its "unfairness" authority by, *inter alia*, prohibiting FTC from using public-policy considerations "as a primary basis for…determin[ing]" that a practice is "unfair." 15 U.S.C. §45(n).

1. Distorted History And Law Cannot Give FTC Data-Security Authority.

FTC distorts the legislative history to serve its power-grab. *See* Opp. 9. It cites "unfair-*competition*" materials from 1914 predating by twenty-four years the 1938 Wheeler-Lea Amendments to the FTC Act, which added "unfair or deceptive acts or practices" to Section 5, and predating by eighty years the 1994 Amendments, which added 15 U.S.C. §45(n). Therefore, FTC's alleged "legislative history" is irrelevant to its Section 5 "unfairness" authority here.[4]

FTC's case authority illustrates only that FTC lacks jurisdiction here. First, none of their cases are legally controlling. FTC admits that no court has ever affirmed its Section 5 authority

[4] FTC cites dicta from *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972), interpreting legislative history from the 1914 pre-Wheeler-Lea Amendments version of Section 5. But Congress was aware of this when it limited FTC's "unfairness" authority in 1994 in 15 U.S.C. §45(n) and overruled FTC's "unfairness" authority claims. *See Miles v. Apex Marine*, 498 U.S. 19, 32 (1990)("Congress…aware of existing law when it passes legislation"). Because *Sperry* was decided over twenty years before §45(n) was enacted, it is irrelevant.

PUBLIC

to regulate patient-information or any other data-security. *Cf.* Mot. 1. Second, none of the cases cited are even factually analogous.

Unlike this case, where LabMD's property was taken by a third party without its knowledge or permission, in *FTC v. Neovi*, the defendant affirmatively participated in fraudulent creation and delivery of unverified checks. *See* 604 F.3d 1150, 1155-57 (9th Cir. 2010). Similarly, in *FTC v. Accusearch*, Accusearch was held liable for maintaining a website selling GPS locations of individual cell phones and other confidential, personal information, where every time Accusearch ordered phone records, they caused use of false pretenses and other fraudulent means to obtain this information. *See* 2007 U.S. Dist. LEXIS 74905, at *17-18 (D.Wyo. Sept. 28, 2007).

Unlike this case, where FTC admits LabMD has always complied with all applicable data-security regulations, *cf.* Mot. at 4,8,13, *Orkin Exterminating Co. v. FTC*—decided years *before* 15 U.S.C. §45(n)'s enactment limiting FTC's "unfairness" authority—involved unilateral breaches of unambiguous contracts through which Orkin wrongfully obtained money from consumers. *See* 849 F.2d 1354, 1363-66 (11th Cir. 1988).

Unlike this case, where FTC admits LabMD has not engaged in any deception, *cf.* Mot. 6, in *FTC v. Verity Int'l, Ltd.*, the defendant not only told its customers they were liable for payments for services they did not use or agree to but "misrepresented…services provided." 335 F. Supp. 2d 479, 484 (S.D.N.Y. 2004).

In re Int'l Harvester Co., 104 F.T.C. 949, 1984 FTC LEXIS 2 (1984), is a Commission decision predating Congress's attempt to rein in FTC via 15 U.S.C. §45(n). It is also factually inapposite. The "unfair" trade practice in that case was a deceptive material omission, i.e., the

PUBLIC

company's failure to warn its customers about serious safety risks associated with its products. *Int'l Harvester*, 1984 FTC LEXIS at *255-62.

2. Congress's Preference for Sector-Specific Data-Security Statutes Trumps the Commission's Data-Security Power-Grab.

FTC again distorts the law, arguing FCRA, GLBA, and COPPA simply provide new "tools," such as "APA rulemaking authority…." Opp. 10. But Section 5 already gives FTC authority to promulgate rules. 15 U.S.C. §57a(a)(1). It just refuses to do so.

FTC also says LabMD "does not grasp the significance of civil penalties" and that under Section 5 FTC can seek only equitable relief. Opp. 11 (citing 15 U.S.C. §45(b)). Yet Section 5 authorizes civil penalties for cease-and-desist order violations of up to $10,000-per-violation, 15 U.S.C. §45(l), *and* authorizes substantial civil penalties for violations of "rules" respecting unfair acts or practices,[5] 15 U.S.C. §45(m).

Finally, FTC says FCRA, GLBA, and COPPA "enhance" FTC's general data-security authority because it need not prove a likelihood of substantial injury thereunder. Opp. 11. But if FTC actually issued data-security rules, as it is both authorized and constitutionally-required to do if Section 5 covered data-security, *see* 15 U.S.C. §57a(a), it would not need to prove substantial injury, 15 U.S.C. §45(m), and would have the same enforcement powers as it does under FCRA, GLBA, and COPPA, thereby rendering these statutes nullities. However, Congress recognized that FTC has no general Section 5 "unfairness" data-security authority and thus enacted these sector-specific statutes. FTC's "enhancement" argument therefore fails.

[5] Civil penalties under subsections (l) and (m) are *four times* higher than those available under the FCRA, 15 U.S.C. §1681s(a)(2)(A); COPPA incorporates FTC Act penalties, 15 U.S.C. §6505(d); and GLBA is enforced under the FTC Act, 15 U.S.C. §6805(a)(7). Thus, the monetary penalty in *U.S. v. Choicepoint*, No. 06-0198 (N.D.Ga. Feb. 15, 2006), was issued "pursuant to…Section(m)(1)(A) of the FTC Act." Stip. Final Judgment 4. Likewise, the Consent Decree in *U.S. v. Path*, No. 13-0448, ¶18 (N.D.Cal. Feb. 8, 2013), expressly states that the civil penalties are imposed "pursuant to Section 5(m)(1)(A) of the FTC Act…."

PUBLIC

C. FTC Disclaimed Authority to Regulate.

Complaint Counsel says "FTC has consistently maintained its ["unfairness" data-security] authority" and that "[a] contrary conclusion requires…tortured application" of a Supreme Court case involving a different agency. Opp. 12. As a matter of fact, this claim straddles the line between distortion and outright deception. As a matter of law, this is breathtakingly wrong.

1. Against the Backdrop of FTC's Admitted Lack of Authority, Congress Enacted Numerous Targeted Data-Security Statutes.

FTC claims that "[s]ince 2000, the FTC has brought nearly fifty data-security cases, more than eighteen of which alleged…unreasonable security is an unfair…practice," citing a string of consent orders. Opp. 12 & n.9. But the *earliest* consent order they cite is dated "Sept. 20, 2005." Opp. 12 n.9. The earliest Commission statements they cite are dated "Mar. 21, 2007" and "Sept. 22, 2004," respectively. Opp. 13 & n.10. Even taking FTC's citations at face value, their world seemingly was created in late 2004.

Furthermore, FTC's out-of-context cherry-picked statement from a footnote in Orson Swindle's testimony must be addressed. *See* Opp. 13 n.10. He never suggested that the Commission has general substantive data-security authority under Section 5, for the very next sentence in footnote 24 states: "[FTC] has used this ["unfairness"] authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing'" and cites two "phishing" cases.

Complaint Counsel does not mention FTC's statement in *Privacy Online: A Report to Congress*, 41 (1998), that FTC generally "lacks authority to require firms to adopt information practice policies," or its statement in *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 34 (2000), that FTC "lacks authority to require firms to adopt

PUBLIC

information practice policies or…abide by…fair information practice principles on their Websites" not directed to children. *Cf.* Mot. 16 n.12. They do not deny that Chairman Pitofsky told Congress the FTC's data-security authority is "limited…to ensuring…Websites follow their stated information practices." Mot. 16 n.12. They offer no response to a FTC official's 2001 statement that "'[t]he agency's jurisdiction is (over) deception….If a practice isn't deceptive,…[FTC] can't prohibit…collecting information." Mot. 16 n.12. They also concede that even FTC's 2008 Resolution did not claim authority to regulate data-security under a pure "unfairness" theory. *Cf.* Mot. 17 n.14.

FTC admits it pestered Congress to confer data-security authority, Opp. 14; *cf.* Mot. 15-16 nn.12-15, but argues that "FTC's requests for additional [data-security] authority showcase…FTC's unfairness authority," Opp. 13. This non-sequitur fails. Asking Congress for the authority to regulate data-security "showcases" only that FTC lacked this authority, for there would be no need to ask for power FTC already had.

FTC's recent statements claiming general Section 5 "unfairness" data-security authority cannot erase FTC's many prior statements disavowing Section 5 data-security jurisdiction or cloud the fact that Congress enacted many targeted data-security statutes against that backdrop.

FTC's reliance on *Smiley v. Citibank*, 517 U.S. 735 (1996), fails. First, here FTC's newfound Section 5 authority is a "[s]udden and unexplained change…." *Id.* at 742. Second, *Smiley* involved an agency regulation entitled to *Chevron* deference. *See id.* at 740-41. No deference is owed to FTC here, because it has not engaged in formal adjudication or rulemaking. *U.S. v. Mead Corp.*, 533 U.S. 218, 227 (2001).

PUBLIC

2. Rejected Legislation Confirms FTC Lacks Authority.

FTC says "savings clauses" in four of *ten* or more bills Congress has rejected that would have given FTC general data-security authority supports its claimed authority. Opp. 14. This is bizarre.

First, all four cited bills were proposed in 2011, Opp. 14, *after* Congress had given FTC sector-specific data-security authority through GLBA, FRCA, and COPPA, Mot. 14 & n.10. Of course, these "[p]reservation clauses would be unnecessary if…FTC lacked existing authority," Opp. 14, under GLBA, FCRA, COPPA, and other targeted statutes. But the "savings clauses" are general, do not refer to Section 5, and protect FTC's data-security authority under these other statutes. *See* S. 1207, §6(d)(protecting "Commission's authority under any other provision of law"); H.R. 2577, §6(d)(same); H.R. 1841, §6(d)(same); H.R. 1707, §6(d)(same). None of these bills address, much less endorse, FTC's claimed Section 5 authority.[6] Indeed, H.R. 2577, §4(d)(1), would have *exempted* HIPAA-covered entities like LabMD from compliance.

Second, FTC ignores *six other* 2011 cybersecurity bills that included no language "preserving" FTC data-security authority. *See* S. 1151, S. 1408, S. 1434, S. 1535, S. 2105, H.R. 624.

D. *Massachusetts v. EPA* Supports LabMD's Arguments.

FTC's reliance on *Massachusetts v. EPA*, 549 U.S. 497 (2007), is misplaced. Unlike Section 5, the Clean Air Act unambiguously defined "air pollutant" to embrace "all airborne compounds of whatever stripe…." *Id.* at 528-29. Moreover, the Court noted two "critical" considerations absent from that case but present in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), and present here. *See Massachusetts*, 549 U.S. at 530-31. First, Section 5

[6] A single Senator's remark during a hearing has no weight, even if it did support FTC.

PUBLIC

data-security jurisdiction for the *entire private economy* is not only "counterintuitive" but leads to "extreme measures," because it would require *substantive* data-security standards for the entire economy to be classified as "unfair" practices and eviscerate Congress's longstanding, deliberate policy of regulating data-security through narrow, targeted statutes. *Cf. id*.

Second, like *Brown & Williamson*, there is "an unbroken series of congressional enactments that ma[k]e sense only if adopted 'against the backdrop of…[FTC's] consistent and repeated statements that it lacked authority'" to regulate data-security. *Cf. id.* For FTC to prevail, Congress's many specific, narrow delegations of data-security regulatory authority enacted against the backdrop of FTC's repeated disavowal of general regulatory authority must be deemed superfluous nullities.[7] Furthermore, unlike *Massachusetts*, many of these statutes, including HIPAA/HITECH, directly conflict with FTC's claimed authority.

E. *ABA v. FTC* Illustrates Why Dismissal Is Required.

FTC dismisses *ABA v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), claiming "there is no debate about the meaning of the term 'unfairness.'" Opp. 16 (citing 15 U.S.C. §45(n)). Given that the one court that actually considered FTC's claimed Section 5 authority to regulate patient-information data-security said "there is significant merit" to LabMD's argument against FTC's power-grab, *see* Mot. 1, and 15 U.S.C. §45(n) does not define "unfairness" but rather cabins FTC's authority,[8] that argument fails.

In truth, FTC concedes that nothing in Section 5 explicitly authorizes it to regulate patient-information data-security practices. Instead, as in *ABA*, FTC is simply grabbing power to "fill in" what it perceives as a regulatory gap. But Congress has already filled that "gap" through

[7] *See* Mot. 11-16 & nn.10-11 (listing and discussing specific statutes).

[8] Statutory language always trumps section titles. *R.R. Trainmen v. Balt.&Ohio R.R.*, 331 U.S. 519, 529 (1947).

PUBLIC

HIPAA/HITECH, and FTC cannot second-guess Congress. FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See ABA*, 430 F.3d at 469-71.

Furthermore, FTC concedes Congress has generally left patient-information data-security to the states, and where Congress has found federal regulation of patient-information data-security practices appropriate, it has explicitly said so. *Cf.* Mot. 21; 42 U.S.C. §1320d-2(d)(1). Because Section 5 does not clearly authorize FTC's conduct here, its brazen power-grab must be denied. *See ABA*, 430 F.3d at 472.

II. FTC'S LACK OF STANDARDS VIOLATES DUE PROCESS.

A. FTC's Admitted Lack of Standards.

FTC admits LabMD has not violated any data-security statutes, rules, or regulations and concedes LabMD has not engaged in a "deceptive" trade practice. *Cf.* Mot. 6,8. It admits LabMD's data-security practices are regulated under HIPAA/HITECH and that HHS exclusively implements and enforces these statutes as applied to LabMD. *Cf.* Mot. 4,13. FTC's sole claim against LabMD is unspecified "unfair" acts or practices. *Cf.* Mot. 7-8.

FTC also admits that Section 5 statutorily bars FTC from enforcing consent orders against non-parties and that its consent orders do not establish illegal conduct and only bind the parties thereto. *Cf.* Mot. 23,26. It has not alleged LabMD had actual notice of the business guides, consumer alerts, links to Sans Institute/NIST publications, and other Internet postings. *Cf.* Mot. 24-28 & nn.19-21. It admits that none of these materials were published in the Federal Register and that *none* of their alleged sources of data-security standards create *any* legally binding duties and obligations. *Cf.* Mot. 7-8. Instead, FTC says Section 5 alone provides

PUBLIC

constitutionally and statutorily adequate *ex ante* notice of what data-security practices are forbidden or required. Opp. 16-17.

B. Section 5 Does Not Establish Proper Standards.

FTC does not acknowledge, much less address, the authorities cited by LabMD holding that FTC was required to provide fair notice of prohibited or required conduct. FTC has never alleged that LabMD's patient-information data-security practices did not meet objective medical-industry standards in effect and applicable to businesses of its size and nature at the time of the alleged violation. *Cf. S&H Riggers & Erectors v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981)(reasonable-person standard divorced from industry standards or regulations violates due process). Instead, FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations. *Cf.* Mot. 4,8,13.

No case has ever held, and no plausible argument can be made, that Section 5 provides constitutionally-adequate data-security fair notice. *See* Stegmaier & Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 706 (2013)("[S]tatutory language does not provide notice of required data-security safeguards."). Section 5's broad "unfairness" prohibition, which does not even refer to "data security," let alone prescribe or proscribe data-security practices, is far more offensive than the statutes at issue in cases like *Connally v. General Constr. Co.*, 269 U.S. 385 (1926)(cited by LabMD but ignored by FTC) finding fair-notice due-process violations. And even if data-security "reasonableness" standards could provide regulated entities with constitutionally-adequate notice if codified in a regulation or statute, FTC says it has not done so and will not do so.

PUBLIC

To claim fair notice, FTC again distorts the law. It cites *U.S. v. Merrill*, 513 F.3d 1293, 1306 (11th Cir. 2008), but this is not a fair-notice case. The cherry-picked portion of *Merrill* it cites discusses *a jury instruction*, not statutory fair notice. Opp. 18. Unlike Section 5, the *Merrill* statute (Controlled Substance Act, 21 U.S.C. §841) is quite detailed and hence provides fair notice.

FTC claims OSHA's General Duty Clause is the best analogy to their standardless *ex post* data-security regime. Opp. 19 n.12. It is a poor fit. Cases interpreting OSHA's General Duty Clause prove LabMD's point and confirm why FTC's actions violate due process, particularly because FTC admits LabMD has always complied with HIPAA/HITECH's specific data-security requirements.

The General Duty Clause is a regulatory tool of last resort—a stop-gap—which "was not meant…[as] 'a general substitute for reliance on standards'" and only applies to "'special circumstances for which no standard has yet been adopted.'" *Ramsey Winch v. Henry*, 555 F.3d 1199, 1205 (10th Cir. 2009). It only controls where there are no other standards, because "standards preempt the [G]eneral [D]uty [C]lause…." *In re Samsonite Corp.*, 756 F. Supp. 498, 500 (D.Colo. 1991). FTC claims that even though LabMD has always complied with HIPAA/HITECH *data-security standards*, it remains liable under Section 5 for compliance with FTC's unstated data-security standards. This is the antithesis of how the General Duty Clause works.[9] *See Teal v. E. I. du Pont*, 728 F.2d 799, 804 (6th Cir. 1984)(Congress "enacted…general duty clause to cover serious hazards…not otherwise covered by specific regulations.").

[9] *See* OSHA's Field Operations Manual, CPL02-00-148, pp.4-14-4-30 (2009)(detailed elements of General-Duty-Clause violation and strict limits). Unlike Section 5, there are 30-plus years of concrete agency guidelines specifying General-Duty-Clause-imposed obligations. *E.g.*, *ConAgra, Inc.*, 1983-84 O.S.H. Dec. (CCH) ¶26,420, 33,523 (1983)(formal agency interpretation).

PUBLIC

The "objective" industry-specific reasonableness standard at issue in *Voegle v. OSHA*, 625 F.2d 1075 (3d Cir. 1980), is fundamentally different from what FTC is doing here. *Voegle* involved a fair-notice challenge to a construction-industry-specific *regulation* (not the General Duty Clause), *see id.* at 1077, far more specific than Section 5's text. Furthermore, *numerous* agency enforcement actions applying occupational-safety regulations far more specific than Section 5 have been dismissed on fair-notice grounds. *E.g.*, *Fabi Const. Co. v. SOL*, 508 F.3d 1077, 1088 (D.C. Cir. 2007); *Gates & Fox v. OSHRC*, 790 F.2d 154,156-57 (D.C. Cir. 1986).

FTC enforcement actions are fundamentally different from garden-variety tort suits, and common-law negligence cases do not displace the APA's and Fifth Amendment's due-process fair-notice requirements. *See Satellite Broadcasting v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987). Also, given FTC admits LabMD has not engaged in "deception," *cf.* Mot. 4, their reliance on dicta from *In re Zappos.com*, No. 12-00325, 2013 U.S. Dist. LEXIS 128155 (D.Nev. 2013), is badly misplaced, for they omit mention of the court's decision to treat the data-security claims as "negligent misrepresentation claims" based on false website statements,[10] *id.* at *15-16.

FTC v. National Urological Group (NUG), 645 F. Supp. 2d 1167 (N.D.Ga. 2008), also deals with "deceptive" advertising allegations not at issue here. FTC itself has explained why "deception" actions do not raise the same fair-notice concerns as "unfairness" actions: "[U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset." *Int'l Harvester*, 1984 FTC LEXIS at *246. Further, the *NUG* court found it critical that, unlike here, FTC had at least expressly defined "competent and reliable scientific evidence" (this definition is omitted from FTC's block-quote) and articulated a definite

[10] *Loschiavo v. City of Dearborn* (overruled) is also not a fair-notice case; inapposite dicta FTC cites refers to the test for whether a private-right-of-action-against-the-government exists under Section 1983. *See* 33 F.3d 548, 551 (6th Cir. 1994).

PUBLIC

standard. *See* 645 F.Supp.2d at 1186. That standard is exponentially more detailed than FTC's proposed "reasonableness" standard here.

Unlike FTC's nebulous, standardless concept of data-security "unfairness," "deception" has a well-established, clear meaning in Section 5 and elsewhere in the law and does not raise the same fair-notice concerns. *E.g.*, FTC Policy Statement on Deception, appended to *Cliffdale Assoc., Inc.*, 103 F.T.C. 110, 174 (1984)(*detailed* explication of deception elements). Thus, "deception" cases cited by FTC do not support its fair-notice argument.

Tellingly, FTC's discussion of the "reasonableness" analysis they believe Section 5 requires contains no citations whatsoever and appears to be cut from whole cloth—the only citation on the page is *In re Zappos.com*, addressed above. Opp. 21.

FTC dismissively argues that "ascertainable certainty does not require agencies to provide…guidance at the level of detail…[LabMD] seems to think appropriate." Opp. 20. They brazenly admit that neither the Complaint nor the notice order prescribe *any* specific data-security practices LabMD *should* (let alone must) implement going forward. *Cf.* Mot. 8. Elsewhere, FTC has boldly stated that the argument that a regulated entity "did not know which standard it was supposed to follow…misses the point." Mot. 27 n.21. They blithely explain that they "do[] not endorse any [industry] standards"—"[they] don't say…how you should set up your router…[they] don't say you should have…white…and black lists for IP addresses"—because "[they] are not tech support." Hearing Transcript, *FTC v. Wyndham*, 53:2-10 (Nov. 7, 2012).

The cases they cite—like the cases LabMD cites to which they do not bother to respond, *see* Mot. 22-28 & nn.19-21—make clear that this violates due process. For example, *U.S. v. Lachman*, 387 F.3d 42 (1st Cir. 2004), which, unlike here, involved a detailed technical

PUBLIC

regulation and interpreted the phrase "specially designed," *id.* at 50-53, notes that the line of D.C. Circuit cases LabMD cites (and FTC ignores) invalidate agency *ex post* enforcement actions where, as here, the statute "is so ambiguous that a regulated party cannot be expected to arrive at the correct interpretation using standard [interpretive] tools…, must therefore look to the agency for guidance, and the agency failed to articulate its interpretation before imposing a penalty," *id.* at 57. Indeed, even FTC's patchwork-quilt of consent orders is inconsistent. *See* Stegmaier & Bartnick, *supra*, at 700 ("FTC has not explained why data-security practices in one [fact-specific consent-order] case may violate Section 5 while those same practices may not violate Section 5 in another case…apparently expect[ing] entities to piece together…complaints and consent orders in thirty-six cases, without any authoritative commentary, to arrive at…[FTC's] interpretation of adequate data-security practices….").

Finally, again without responding to LabMD's arguments and thereby conceding the points, *cf.* Mot. 25-26 & n.19, FTC—incredibly—suggests that NIST and HIPAA publications supply standards LabMD should have followed. Opp. 22 n.15. The NIST Handbook they cite is from 1995, does "not…specify requirements," and only "provides a broad overview of computer security." NIST, Special Publication, 800-12, §1.1 (1995). Section 1.1 of NIST Special Publication 800-30 states: "The guidelines herein are not mandatory and binding standards." With respect to HIPAA Guidance they cite, even if LabMD was required to follow it, FTC has admitted that LabMD *has always complied with all data-security obligations under HIPAA/HITECH.*

C. FTC Cannot Announce New Rules Through Adjudication Punishing Past Conduct.

The fact that, subject to fair notice, FTC may fill in Section 5's interstices through adjudication does not allow FTC to deliberately evade its constitutional and statutory fair-notice

PUBLIC

obligations. FTC cannot regulate through intimidation by bullying companies into signing consent decrees. Yet FTC brags about the myriad consent decrees secured from 2005 to present, Opp. 12-13 n.9, and says they are "not obligated to engage in a rulemaking…," Opp. 23. *SEC v. Chenery*, 332 U.S. 194 (1947), where, unlike here, the agency "had not previously been confronted with the problem," *id.* at 203, explains that "[t]he function of filling in…[statutory] interstices…should be performed, as much as possible, through…quasi-legislative promulgation of rules to be applied in the future," *id.* at 202. *Chenery* is not a fair-notice case; unlike here, SEC did not seek liability for past conduct, *see id.* at 203-04. *PBW Stock Exch. v. SEC*, 485 F.2d 718 (3d Cir. 1973), also not a fair-notice case, involved *a challenged regulation*, not adjudication, *id.* at 721; dicta FTC cites is inapposite.

In *Beazer v. EPA*, 963 F.2d 603 (3d Cir. 1992), EPA had actually promulgated regulations through normal notice-and-comment rulemaking and the statute and regulations prescribed detailed requirements, *see id.* at 604-05. In that context, the court found adjudication permissible. *Cf. id.* at 609 (APA "expressly prohibit[s]…agency from retroactively imposing…interpretive rule upon…regulated party."). Unlike *Beazer*, here FTC brazenly admits that they do not have legislative or even interpretive rules explaining what data-security practices they believe Section 5 forbids or requires. *Cf. id.* at 606.

NLRB v. Bell Aerospace, 416 U.S. 267 (1974), is not a fair-notice due-process case and thus inapposite. Rather, the issue was Bell Aerospace's *future* collective-bargaining obligations. *See id.* at 269. Even in that very different context, the Court recognized situations where NLRB reliance on adjudication would be unlawful, noting that "this is not a case in which some new liability is sought to be imposed…for past actions" and that "fines or damages" were not involved. *Id.* at 294-95. Due-process-based fair-notice requirements are heightened where, as

PUBLIC

here, the agency alleges violation of law based on *past* conduct. *See PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000).

III. FTC'S FAILURE TO STATE PLAUSIBLE SECTION 5 VIOLATION.

FTC concedes it lacks even *one* complaining witness who has suffered *any* injuries because of LabMD's alleged patient-information data-security failures. FTC admits LabMD complied with HIPAA/HITECH—the only applicable patient-information data-security requirements. FTC does not allege what the objective medical-industry-standard data-security practices are or were or that LabMD's data-security practices fell short of meeting them. As explained above, the *Iqbal/Twombly* standard applies here. The Complaint fails to meet that standard and must be dismissed.

IV. STAY NECESSARY TO STOP DISCOVERY ABUSE.

FTC does not deny that its discovery tactics are barred in federal courts and does not substantively respond to LabMD's arguments or deny LabMD's assertions. At minimum, the Commission should stay the proceedings.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion in full.

PUBLIC

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com
Senior Vice President for Litigation and
Counsel to Cause of Action

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Dated: December 2, 2013

PUBLIC

CERTIFICATE OF SERVICE

I hereby certify that on December 2, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: December 2, 2013 By: /s/ Michael D. Pepson

EXHIBIT 25

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Terrell McSweeny

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**

ORDER DENYING RESPONDENT LABMD, INC.'S
MOTION FOR SUMMARY DECISION

By Commissioner Joshua D. Wright, for a unanimous Commission:[1]

Respondent LabMD, Inc. ("LabMD") seeks a summary decision dismissing with prejudice the Complaint in this matter. Motion for Summary Decision, filed April 21, 2014 ("Motion"). It argues that there is "no genuine dispute as to any material fact regarding liability or relief" in this case, and that we should proceed to "issue a final decision and order" in LabMD's favor. Motion at 8 (quoting 16 C.F.R. § 3.24(a)(2)). Complaint Counsel opposes that request.[2] We find that there are genuine disputes about some of the facts asserted by LabMD in its Motion, and that other such facts are not material to the ultimate question of whether LabMD is liable for engaging in "unfair acts or practices" in violation of Section 5(a) of the Federal Trade Commission Act ("FTC Act), 15 U.S.C. § 45(a). That question must be resolved based on factual evidence presented at an evidentiary hearing. Accordingly, we deny LabMD's Motion for Summary Decision.

BACKGROUND

On August 28, 2013, the Commission issued an administrative Complaint commencing this adjudicatory proceeding. The Complaint alleges that LabMD's data security practices, "taken together, failed to provide reasonable and appropriate security for personal information

[1] Commissioner Brill did not take part in the consideration or decision herein.

[2] *See* Complaint Counsel's Response in Opposition to Respondent's Motion for Summary Decision, filed May 5, 2014 ("CC Opp."); Complaint Counsel's Separate and Concise Statement of Material Facts as to Which There Exist Genuine Issues for Trial, filed May 5, 2014 ("CC Stmt."). *See also* LabMD Reply in Support of Motion to Dismiss, filed May 12, 2013 ("LabMD Reply").

stored on its computer networks," even though LabMD "could have corrected its security failures at relatively low cost using readily available security measures." Complaint, ¶¶ 10, 11. The Commission thus found "reason to believe" that LabMD's conduct could constitute "unfair . . . acts or practices" in violation of 15 U.S.C. § 45(a), and determined that an adjudicatory proceeding would be "in the public interest." *Id.*, Preamble & ¶¶ 22-23 (quoting 15 U.S.C. § 45(b)).

The Complaint sets forth specific allegations of "reasonable and appropriate" data security measures that LabMD allegedly should have implemented, but failed to implement, to minimize the risk of security breaches. Complaint, ¶¶ 10(a)-(g), 11. The Complaint goes on to allege that LabMD experienced two security breach incidents. First, unauthorized third parties allegedly retrieved a June 2007 "insurance aging report" and possibly other files containing sensitive consumer information from LabMD's computer systems via Limewire, a peer-to-peer file-sharing application that was installed on the computer of LabMD's billing manager. *Id.*, ¶¶ 17-20. Second, the Sacramento Police Department discovered identity thieves in possession of LabMD "day sheets" containing personal information and consumer checks payable to LabMD. *Id.*, ¶ 21.

The Complaint charges (1) that LabMD's purported data security failures caused, or were likely to cause, harm to consumers, including "identity theft, medical identity theft, and . . . disclosure of sensitive, private medical information" and other personal information including addresses, telephone numbers, social security numbers, bank account and credit card numbers. *Id.*, ¶¶ 6, 9, 12, 19, 21, 22; (2) that consumers could not have learned about LabMD's data security practices or avoided these potential injuries independently, *id.*, ¶ 12; and (3) that LabMD's alleged data security failures did not substantially benefit LabMD or anyone else, *id.*, ¶¶ 11, 20, 22.

In its Answer to the Complaint and Affirmative Defenses, filed September 17, 2013 ("Answer"), and its Objections and Responses to Complaint Counsel's Requests for Admission pursuant to 16 C.F.R. § 3.32, filed March 3, 2014 ("LabMD Admissions/Denials"), LabMD admits most, but not all, of the Complaint's allegations regarding the nature of its business, the services it provides, and the types of consumer information stored on its computer systems. *See* Answer, ¶¶ 1, 3-6, 8-9; LabMD Admissions/Denials, ¶¶ 1-13, 16-28, 35-38.[3] LabMD admits that Limewire had been installed on a computer used by its billing manager and that a company called Tiversa, Inc. had obtained access to LabMD's June 2007 insurance aging report. But in other respects, LabMD either denies, or pleads insufficient knowledge to admit or deny, most of the charges concerning the Limewire and Sacramento data breach incidents. Answer, ¶¶ 17-20; LabMD Admissions/Denials, ¶¶ 39-49. LabMD denies the Complaint's allegations concerning the list of specific data security measures that it did not implement. Answer, ¶¶ 10-11. It also generally denies the allegations regarding the causal relationship between its conduct and actual or potential consumer injury, and whether such injury was avoidable by consumers or whether its conduct had any countervailing benefits. *Id.*, ¶¶ 11-12, 22-23.

[3] LabMD denies that it maintained electronic copies on its computer networks of patients' checks, Answer, ¶ 9(c); LabMD Admissions/Denials, ¶¶ 33-34; and it takes issue with the allegations concerning the number of laboratory tests and the number of affected consumers. Answer, ¶ 7; LabMD Admissions/Denials, ¶¶ 14-15, 19-20.

On November 12, 2013, LabMD filed a motion to dismiss the Complaint. It contended that (1) the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the FTC Act; (2) the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security implicitly strip the Commission of authority to enforce Section 5 in the field of data security; and (3) due process requires the Commission to adopt regulations governing data security before we may engage in an enforcement action. The Commission rejected those arguments and denied the motion. *See* Order Denying Respondent LabMD's Motion to Dismiss (issued January 16, 2014) ("MTD Denial Order").

From December 2013 through April 2014, LabMD and Complaint Counsel engaged in discovery concerning factual issues and expert testimony, including extensive document production, depositions, and requests for admissions. This Motion for Summary Decision followed.

STANDARD OF REVIEW

We review LabMD's Motion for Summary Decision pursuant to Rule 3.24 of our Rules of Practice, 16 C.F.R. § 3.24, whose "provisions are virtually identical to the provisions of Fed. R. Civ. P. 56, governing summary judgment in the federal courts." *N.C. Bd. of Dental Examiners*, 151 F.T.C. 607, 610-11 (2011); *see also Hearst Corp.*, 80 F.T.C. 1011, 1014 (1972). A party moving for summary decision must show that "there is no genuine dispute as to any material fact," and that it is "entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).

"[T]he substantive law will identify which facts are material . . . . [*i.e.*, those] that might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby*, 477 U.S. 242, 248 (1986). Here, the applicable substantive law is Section 5(n) of the FTC Act, which deems an act or practice to be "unfair" if it [1] "causes or is likely to cause substantial injury to consumers"; [2] such injury "is not reasonably avoidable by consumers themselves"; and [3] such injury "is not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). Facts are "material" for present purposes only if they tend to prove or disprove that LabMD's data security practices satisfy one or more of these criteria. Facts that have no bearing on these dispositive questions "are irrelevant or unnecessary [and] will not be counted." *Anderson*, 477 U.S. at 248.

There is no "genuine" dispute over material facts where the "evidence favoring the non-moving party . . . is merely colorable, [but] not significantly probative." *Id.* at 249. The "party seeking summary judgment always bears the initial responsibility of . . . identifying" factual information in the record that "it believes demonstrate[s] the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). Where, as here, the party opposing the motion bears the ultimate burden of proof, *see* 16 C.F.R. § 3.43(a) (imposing burden of proof on Complaint Counsel), the moving party may "discharge this initial responsibility" either by showing that "there is an absence of evidence to support the non-moving party's case" or by supplying "affirmative evidence demonstrating that the non-moving party will be unable to prove its case at trial." *Fitzpatrick v. City of Atlanta*, 2 F.3d 1112, 1115-

16 (11th Cir. 1993). "Only when that burden has been met does the burden shift to the non-moving party to demonstrate that there is indeed a material issue of fact that precludes summary judgment." *Clark v. Coats & Clark, Inc.*, 929 F.2d, 604, 608 (11th Cir. 1991); *see also* 16 C.F.R. § 3.24(a)(3) ("When a motion for summary decision is made and *supported as provided in this rule*, a party opposing the motion . . . must set forth specific facts showing that there is a genuine issue of material fact for trial.") (emphasis added). "On summary judgment the inferences to be drawn from the underlying facts must be viewed in the light most favorable to the party opposing the motion." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (citation omitted).

ANALYSIS

I. GENUINE ISSUES OF MATERIAL FACT

In a section of its Motion entitled "Statement of Facts," LabMD sets forth facts that it contends are both "material" and not subject to "genuine" dispute. *See* Motion at 4-8 ("LabMD Stmt."); *cf.* 16 C.F.R. § 3.24(a). We consider the assertions in each of the 24 paragraphs in this Statement,[4] as well as factual assertions set forth in other sections of LabMD's Motion, to determine (1) whether they constitute "material" facts; (2) if so, whether there is no "genuine" dispute about them; and (3) whether, on that basis, LabMD is entitled to a summary decision in its favor as a matter of law.

A. HIPAA Data Security Standards

LabMD asserts that "[a]ll information received, utilized, maintained and transmitted by LabMD is protected health information ('PHI') as defined by the Health Insurance Portability and Accountability Act of 1996 ('HIPAA')." Motion at 1 (citing 45 C.F.R. § 160.103).[5] LabMD's Statement of Facts includes five paragraphs relating to the data security requirements imposed by HIPAA and related statutes and rules (collectively, "HIPAA Standards"), and characterizes that text as a set of "material" facts that are not in "genuine" dispute.[6]

[4] We refer to each of these paragraphs using the convention "[X.Y]," where X refers to the page number of the Motion and Y refers to the position of the paragraph in sequence of the paragraphs beginning on that page. Thus, "LabMD Stmt. 5.2" refers to the second full paragraph on page 5 of the Motion.

[5] Significantly, LabMD does not assert that the scope of personal health information included in the definition of "PHI" is co-extensive with the scope of the "personal information" at issue here, as defined in the Complaint (¶ 6), nor does it refer to any evidence or legal authority that would support that proposition.

[6] *See* LabMD Stmt. 4.2 ("LabMD is a "Covered Entity" that receives, maintains and transmits PHI during the normal course of its business."); *id.* 5.5 ("LabMD is a HIPAA-covered entity. . . . It must comply with HHS's HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations . . . ."); *id.*, 5.6 ("HIPAA's Security Rule establishes substantive data-security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply."); *id.* 5.7 ("HHS exclusively enforces HIPAA and HITECH. . . ."); *id.*, 6.1 ("The FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations. . . .").

LabMD further contends that Complaint Counsel's expert witness, Dr. Raquel Hill, articulated data security standards pursuant to Section 5 "that are difficult to reconcile with," and are "far more stringent" than, the HIPAA Security Rule and other HIPAA Standards. Motion at 3, 20. For example, LabMD asserts that Dr. Hill's proposed standards "do not account, as required by HIPAA, for the needs and capabilities of small health care providers and rural health care providers," improperly "presume a level of technical knowledge generally not available to small health care providers," and are "inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process." *Id.* at 21. From those asserted facts, LabMD contends that its "compliance with the HIPAA [Standards]" should not be deemed "irrelevant to . . . Section 5 unfairness claims," but rather should be a complete "defense" to such claims. *Id.* at 20.

Complaint Counsel responds that LabMD's asserted facts relating to HIPAA "are irrelevant or immaterial" and that it need not "demonstrate that [LabMD's] conduct violated other laws in order to establish that [LabMD's] practices were unfair under Section 5." CC Opp. at 4. Complaint Counsel contends that "the Commission [has] already rejected the argument that the FTC Act and HIPAA are at odds," *id.* at 12 (citing MTD Denial Order at 12), and asserts that LabMD's arguments "that the FTC's data security 'standards' are not scalable or presume too high a level of technical knowledge for small health care providers should be addressed at trial and do not support a summary decision." *Id.*

We conclude that LabMD's factual contentions regarding HIPAA data security standards do not justify a summary decision in LabMD's favor. As LabMD concedes, "[t]he FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations," Motion at 6 (LabMD Stmt. 6.1), and "this case has nothing to do with HIPAA." *Id.* at 10 (quoting MTD Denial Order at 12). Rather, this case concerns LabMD's compliance with Section 5 of the FTC Act. Thus, the facts that LabMD alleges about HIPAA could be "material" for purposes of this Motion for Summary Decision only if LabMD were correct that, as a matter of law, the Commission could not hold LabMD liable under Section 5 if its data security practices complied with HIPAA Standards. Motion at 1. But that legal argument is now foreclosed. We held in the Order denying LabMD's Motion to Dismiss that HIPAA does not "trump" Section 5, and that LabMD therefore "cannot plausibly assert that, because it complies with [HIPAA], it is free to violate" requirements imposed independently by Section 5 of the FTC Act. MTD Denial Order at 11, 13; *see infra*, Part II.[7]

In any event, LabMD's statements of fact regarding HIPAA Standards would be insufficient to merit summary decision in its favor even if, counterfactually, those Standards *did* define the scope of Section 5 liability as a matter of law. LabMD points to no record evidence regarding what measures, if any, it implemented to prevent data breaches. It does not explain which HIPAA Standards apply to LabMD's actions or why LabMD's conduct satisfied them. Indeed, LabMD does not even assert that it *complied* with the applicable HIPAA Standards; it merely avers that the Commission has not accused it of *violating* those requirements. *See, e.g.,*

[7] Consistently, HHS, in adopting regulations implementing HIPAA, recognized that entities subject to HIPAA "may be required by other Federal law to adhere to additional or more stringent security measures," and consequently, that "[s]ecurity standards in [HHS's] final rule establish a minimum level of security that covered entities must meet." Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8355 (Feb. 20, 2003).

LabMD Stmt. 6.1. The "party seeking summary judgment bears the initial responsibility of informing the [adjudicator] of the basis for its motion, and identifying those portions of the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, which it believes demonstrate the absence of a genuine issue of material fact." *Celotex*, 477 U.S. at 323 (quotation marks omitted). LabMD has not carried this burden.[8]

In sum, because we conclude that LabMD's HIPAA-related factual assertions are not "material" to the violations of law alleged in the complaint and, in any event, are not supported by any evidence, we need not determine whether they are in "genuine" dispute.

B. Alleged Limewire and Sacramento Security Breaches

LabMD identifies what it characterizes as "material" facts regarding the two specific security breaches alleged in the Complaint – *i.e.*, the alleged breach relating to the installation of Limewire on a billing computer,[9] and the alleged breach discovered by the Sacramento Police Department.[10]

We conclude that these factual claims, even if undisputed, are not material and would not support a summary decision in LabMD's favor. LabMD has not attempted to show how its factual assertions regarding the Limewire and Sacramento incidents are material to its liability as alleged in the Complaint. For example, even if we accepted as true the claims that Tiversa retrieved the Insurance Aging File without LabMD's knowledge or consent (LabMD Stmt. 4.3), that Tiversa improperly passed on that file to Professor Johnson or others (*id.*, 4.5), and that Tiversa touted its unique technology (*id.*, 4.3 n.2), these facts would not resolve the ultimate questions we must decide in this case. In particular, they would not compel us, as a matter of

[8] We cannot determine, on the present record, whether, in fact, LabMD *has* complied with or violated HIPAA Standards. For purposes of the present Motion, we must draw all reasonable inferences in support of the party opposing the Motion—*i.e.*, Complaint Counsel—and consequently, we cannot infer from LabMD's unsupported assertions that it complied with applicable HIPAA Standards. Moreover, we express no view on whether and to what extent such compliance or noncompliance might be a relevant factor in our assessment of whether LabMD violated Section 5. We agree with Complaint Counsel that any such arguments "should be addressed at trial." CC Opp. at 12.

[9] *See* LabMD Stmt. 4.3 ("On or about February 5, 2008, without LabMD's knowledge or consent, Tiversa, Inc. ('Tiversa'), took possession of a single LabMD insurance aging file (the 'Insurance Aging File')."); *id.* n.2 ("Tiversa has testified before Congress that it possesses unique technology which among other things allows it to download computer files from unsuspecting third persons inadvertently sharing computer files via peer to peer ('P2P') networks."); *id.*, 4.4 ("The Insurance Aging File contained PHI for over 9,000 patients of LabMD's physician clients."); *id.*, 4.5 ("Subsequently, Tiversa made the Insurance Aging File available to Professor Eric Johnson, of Dartmouth College, who was conducting research under a government contract for his article entitled, 'Data Hemorrhages in the Health Care Sector'."); *id.*, 4.6 ("In January 2010, the FTC began a three year full investigation of LabMD's data security practices based upon the disclosure of the PHI contained in the Insurance Aging File.").

[10] *See* LabMD Stmt. 5.1, 5.2, and 5.3 ("In October 2012, during a raid of a house of suspected identity thieves, the Sacramento Police Department found LabMD 'day sheets' and copies of checks made payable to LabMD. Again, the day sheets and checks contained PHI from patients of LabMD's physician clients."); *id.* 5.2 ("In an attempt to notify LabMD of its find, the Sacramento police 'googled' LabMD, and discovered that LabMD was under investigation by the FTC."); *id.*, 5.3 ("The Sacramento police then notified the FTC of its find, but did not notify LabMD, despite Sacramento's awareness of LabMD's duty to notify under HIPAA.").

law, to dismiss the allegations in the Complaint that LabMD failed to implement reasonable and appropriate data security and that such failure caused, or was likely to cause, unavoidable and unjustified harm to consumers. To the contrary, LabMD's factual contentions concerning Tiversa and the Sacramento Police Department are fully consistent with the Complaint's allegations that LabMD failed to implement reasonable and appropriate data security procedures.

C. Genuine Disputes Over Reasonable and Appropriate Data Security Practices

LabMD raises a number of contentions that could be construed as addressing issues of material fact, but it fails to demonstrate that there is no "genuine dispute" over these issues. For example, LabMD criticizes the opinions of Complaint Counsel's expert witness concerning appropriate data security measures. *See* Motion at 13, 16, 18, 20-22; *id.*, Exh. 5. The issues addressed by this expert report are undoubtedly material. But there is plainly also a genuine dispute about them. Indeed, LabMD submitted the declaration of its own expert witness, whose report conflicts with that of Complaint Counsel's expert witness.[11] *See* Motion, Exh. 12; *see also* Motion at 22; LabMD Reply at 11-13. Such conflicting expert opinion is precisely the type of dispute that evidentiary hearings are held to resolve.

Similarly, LabMD's Statement asserts, "The FTC has never specified what data security standards were in place at any given point during the relevant time period or when LabMD specifically violated them." LabMD Stmt. 6.4. This contention could be read as encompassing both factual and legal issues,[12] of which at least some are genuinely disputed.[13] We cannot resolve such disputes on the present record, and LabMD has not shown, with respect to this contention, that it is entitled to judgment as a matter of law.

[11] We decline to address Complaint Counsel's request that we strike Mr. Baker's declaration on the grounds that LabMD "did not timely designate Mr. Baker [as an expert] in this proceeding and its use of his declaration contravenes the Scheduling Order." CC Opp. at 4 n.2. The Commission (or the ALJ) may consider a Motion to Strike if submitted as a stand-alone pleading, rather than as a footnote to a brief regarding another motion.

[12] It is unclear whether LabMD, in using the term "the FTC" in Stmt. 6.4, intends to refer to Complaint Counsel or to the Commission. To the extent LabMD is contending that Complaint Counsel, in the course of this adjudication, has yet to identify with specificity what data security standards it alleges LabMD violated, this contention is not a material fact because the adjudication is still underway and, as discussed below, the Commission is not bound by Complaint Counsel's arguments or characterizations. *See infra* notes 15-18 and accompanying text. To the extent LabMD's statement is simply an alternative formulation of its legal argument that the Commission infringed its Constitutional due process rights by providing inadequate advance notice, the statement is unavailing because we have already rejected that legal argument. *See infra* Section II; *see also* MTD Denial Order at 14-17 (rejecting LabMD's due process/fair notice argument); Motion at 11-18 (rearguing the same legal claim); LabMD Reply at 3-12 (same). We recognize that there may be other ways to interpret LabMD's statement that might implicate unresolved legal questions or material issues of fact; but for present purposes, we cannot draw inferences in LabMD's favor.

[13] *Compare* LabMD Stmt. 6.4, 6.5, and 7.1 *with* CC Stmt. ¶¶ 1-10 (and evidence cited therein) (genuine factual disputes over applicable standards and LabMD's conduct). *See also* LabMD Reply at 6-9 (citing and disputing legal arguments in Complaint Counsel's Pre-Trial Brief (filed May 6, 2014)).

D. Other Immaterial Matters

We conclude that the remaining factual assertions in LabMD's Statement of Facts are immaterial. First, the procedural history of this case, even if undisputed, does not support any particular conclusion on whether LabMD's conduct violated the FTC Act.[14]

In addition, the propositions cited in LabMD's Statement of Facts characterizing the Commission's positions on the basis of Complaint Counsel's statements to the Administrative Law Judge during an Initial Pretrial Conference,[15] Complaint Counsel's responses to LabMD's discovery demands[16] and requests for admissions,[17] and Complaint Counsel's objections to questions posed during a deposition,[18] do not constitute facts at all, let alone material facts. Just because Complaint Counsel has made particular statements or taken certain positions does not necessarily mean *the Commission* has adopted those positions. To the contrary, the Commission is not bound by characterizations employed by Complaint Counsel, and is free to reject Complaint Counsel's arguments or reject its evidence. Moreover, the statements of counsel cited by LabMD are not contained in sworn affidavits or testimony, as required under 16 C.F.R.

[14] *See, e.g.,* LabMD Stmt. 4.6 ("In January 2010, the FTC began a three year full investigation of LabMD's data security practices . . . ."); *id.,* 5.4 ("In August, 2013, FTC filed an Administrative Complaint."); *id.,* 6.2 ("The FTC alleges that LabMD's data-security is inadequate to protect the PHI it possesses and that this failure to adequately protect PHI is an unfair practice affecting consumers in violation of Section 5 of the Federal Trade Commission Act.").

[15] *See* LabMD Stmt. 6.6 ("When asked by the ALJ whether 'the Commission issued guidelines for companies to utilize to protect...[sensitive] information or is there something out there for a company to look to,' the FTC admitted that '[t]here is nothing out there for a company to look to.'"); *id.,* 7.1 ("The FTC admits that it has never promulgated data-security regulations, guidance, or standards under Section 5: '[T]here is no rulemaking, and no rules have been issued . . . .'"); *id*., 7.2 ("When asked about other sources of data-security standards, FTC said, the 'Commission has entered into almost 57 negotiations and consent agreements that set out . . . the method by which the Commission assesses reasonableness.' . . . . And finally the FTC argued that 'the IT industry has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology . . .,' except that the 'Commission's process' involves 'calculation of the potential consumer harm from unauthorized disclosure of information.'"); *id.,* 8.1 ("At the hearing, the ALJ asked: 'Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?' The FTC responded 'No.'"); *id.,* 8.2 ("The FTC also admits that '[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward.'") (quoting colloquy between Complaint Counsel Alain Sheer and Chief Administrative Law Judge D. Michael Chappell, Transcript of Initial Pretrial Conference, September 25, 2013).

[16] *See* LabMD Stmt. 7.3 ("In response to LabMD's written discovery requesting documents relating to the standards the FTC enforces regarding data-security, the FTC produced thousands of pages of consent decrees, reports, PowerPoint presentations, and articles from the FTC's website, including many in Spanish.") (citing attachments to letters from Complaint Counsel transmitting responses to LabMD document requests).

[17] *See* LabMD Stmt. 6.5 ("The FTC claims it need not 'allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use.'") (quoting Complaint Counsel's Amended Response to LabMD's First Set of Requests for Admission (filed as Exh. B to Complaint Counsel's Motion to Amend Complaint Counsel's Response to Respondent's First Set of Requests for Admission)).

[18] *See* Motion at 14 ("Respondent's counsel asked [FTC Bureau of Consumer Protection Deputy Director Daniel] Kaufman a series of questions related to published standards that the Bureau sought to enforce against LabMD; however, Complaint Counsel instructed the witness not to respond to any of these questions.") (citing Deposition of Daniel Kaufman, April 14, 2014).

§ 3.24(a)(3) & (4), and thus are little more than "mere allegations or denials," 16 C.F.R. § 3.24(a)(3), which can neither support nor defeat a Motion for Summary Decision.

Most significantly, even if these statements or arguments of Complaint Counsel could be construed as facts, and even if they were not genuinely in dispute, they still would not be material to this case. The statements and arguments of Complaint Counsel that LabMD lists in its Statement of Facts relate primarily to LabMD's legal arguments concerning due process, jurisdiction, and related matters, which we already rejected in our Order denying LabMD's Motion to Dismiss. *See infra*, part II. They appear to have little, if any, bearing on the open issues affecting our decision on whether LabMD's data security practices violated Section 5.

Finally, LabMD's contention that it "owns" the consumer information at issue also is immaterial. *See* Motion at 9-10. LabMD contends that "the PHI in LabMD's possession is information that patients voluntarily gave to their doctors, who in turn, voluntarily provided this information to LabMD," and thus, that the information at issue is LabMD's "own property." *Id.*[19] The central questions to be decided here are whether LabMD's data security practices were reasonable and whether they caused, or were likely to cause, significant injury to consumers that was unavoidable and unjustified by offsetting benefits. Those questions do not turn on the "ownership" of the data. It is quite possible that a company could use (or misuse) its "own property" in a manner that causes, or is likely to cause, significant harm to others. If such misuse satisfies the criteria of Section 5, it may constitute an "unfair act or practice."

II. LABMD'S RENEWED DUE PROCESS AND JURISDICTIONAL CHALLENGES

LabMD asserts that we wrongly denied its Motion to Dismiss, Motion at 8, and implicitly asks us to reconsider the issues raised in that Motion. We decline to do so. We have already carefully addressed and disposed of LabMD's arguments that (1) its due process rights were infringed and that it lacked adequate notice of what conduct is prohibited (*compare* Motion at 11-12, 15-16, and LabMD Reply at 4-6, *with* MTD Denial Order at 16-17); (2) the Commission cannot bring enforcement actions to address statutory violations unless it has adopted specific rules or announced detailed compliance standards in advance (*compare* Motion at 13-18 and LabMD Reply at 6-10, *with* MTD Denial Order at 14-17); and (3) HIPAA supersedes any FTC authority over unfair data security practices and that HIPAA and the FTC Act are in irreconcilable conflict (*compare* Motion at 18-20, and LabMD Reply at 13-15, *with* MTD Denial Order at 10-13).

[19] In support of this assertion, LabMD contends that, as a matter of law, "consumers who voluntarily provide personal information to third parties lose their privacy rights because the information in question once given, belongs to the receiver and not the consumer." Motion at 9. LabMD therefore rejects what it characterizes as "FTC's foundational premise"—that "consumers who voluntarily give PHI to medical providers have some protectable privacy or other interest in that information beyond that which Congress authorized HHS to carve out under HIPAA." *Id.* at 10. *See also* CC Opp. at 8 & n.3 (opposing argument). For present purposes, we need not resolve the merits of this novel legal proposition.

We need not reiterate the legal analysis set forth in our earlier Order. LabMD identifies no "new questions raised by the decision . . . upon which [it] had no opportunity to argue," *see* 16 U.S.C. § 3.55; and even if it had done so, it failed to submit a Petition for Reconsideration within 14 days of the service of our Order. *Id.* To the extent LabMD continues to disagree with the legal conclusions set forth in that interlocutory decision, it may seek judicial review pursuant to 15 U.S.C. § 45(c)-(d)—but *only* if and when we issue a final order against LabMD at the conclusion of this adjudicatory proceeding. *See, e.g., FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232 (1980).[20] We express no view on the open legal questions at issue in this proceeding, or on the numerous, genuinely disputed issues of material fact that have not yet been resolved.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion for Summary Decision **IS DENIED.**

By the Commission, Commissioner Brill not participating.

Donald S. Clark
Secretary

SEAL:
ISSUED: May 19, 2014

[20] *See also LabMD, Inc. v. FTC*, No. 13-15267-F (11th Cir. Feb. 18, 2014) (*per curiam*) (dismissing challenge to adjudicatory proceeding for lack of jurisdiction, because no cease and desist order had been issued); *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD (N.D. Ga. May 12, 2014) (same), *appeal pending*.

EXHIBIT 26

PUBLIC
PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
11 12 2013
SECRETARY

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
	)	**PUBLIC**
LabMD, Inc.,	)	
a corporation.	)	**ORAL ARGUMENT REQUESTED**

RESPONDENT LabMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

PUBLIC

TABLE OF CONTENTS

INTRODUCTION 1

STATEMENT OF FACTS 4

STANDARD OF REVIEW 8

ARGUMENT 9

I. The Commission Lacks Section 5 "Unfairness" Authority to Regulate Patient-Information Data-Security Practices. 9

A. Congress Authorized HHS, Not The FTC, To Regulate Patient-Information Data-Security Practices. 10

1. Controlling interpretative canons hold the FTC's general Section 5 authority (if any) must yield to the specific patient-information statutes and regulations. 10

2. The *Billing* doctrine controls and so the FTC has no authority. 13

B. Congress Has Not Given The FTC The Plenary Power To Regulate Data-Security Through Its Section 5 "Unfairness" Authority. 14

1. The FTC's claim of general Section 5 "unfairness" authority to regulate data-security practices is contradicted by Congress's many specific data-security delegations. 14

2. The Commission's claim of Section 5 "unfairness" authority to regulate data-security economy wide is contrary to congressional intent and to controlling Supreme Court authorities. 16

C. *ABA v. FTC* Stands For Dismissal. 20

II. The Commission Has Failed to Give Fair Notice of What Data-Security Practices It Believes Section 5 Forbids or Requires Thereby Violating LabMD's Due Process Rights 22

A. Due Process Requires Fair *Ex Ante* Warning of Prohibited or Required Conduct. 22

B. The Commission Has Denied LabMD Fair Notice 23

1. The Commission has wrongfully failed to provide *ex ante* notice through regulations.. 23

2. The FTC's alleged "standards" are legally meaningless. 24

III. The Acts or Practices Alleged in the Complaint Do Not Affect Interstate Commerce. ... 28

IV. The Complaint Does Not Comply with the Commission's Pleading Requirements. 28

V. This Matter Should Be Stayed Pending Disposition of this Motion..... 29

CONCLUSION 30

PUBLIC

RESPONDENT LabMD, INC'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

Please take notice that, pursuant to Commission Rule 3.22(a), 16 C.F.R. § 3.22(a), Respondent LabMD, Inc. (LabMD), hereby moves to dismiss the Federal Trade Commission's (the "Commission" or "FTC") Administrative Complaint (the "Complaint") in its entirety with prejudice and to stay all proceedings before the Administrative Law Judge (ALJ) pursuant to Commission Rule 3.22(b), 16 C.F.R. § 3.22(b), while this Motion is under review.

INTRODUCTION

The only federal court to address the legitimacy of the FTC's claimed authority to regulate data-security practices as "unfair" acts or practices under Section 5 of the Federal Trade Commission Act (FTCA), 15 U.S.C. § 45, said "there is significant merit" to the argument that Section 5 does not provide general jurisdiction over data-security practices and consumer-privacy issues.[1] *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7 (N.D. Ga. Nov. 26, 2012). When asked to cite a case that "says the FTC has the authority to investigate data security under Section 5," a Commission attorney admitted that "I cannot point you to that case. It doesn't exist…." Hearing Transcript, *FTC v. LabMD*, No. 1:12-cv-3005-WSD, at 16:20-25 (N.D. Ga. Sept. 19, 2012).

[1] The court, noting its "sharply limited" role, explained that the "subpoena enforcement proceeding is not the proper forum" to decide the scope of statutory jurisdiction. *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7. It only found that the FTC had made a "plausible" argument that it had jurisdiction to *investigate* whether LabMD had engaged in unfair or deceptive practices. *Id.* at 1-2, 6-7, 12-13 & n.3. Notably, the FTC's Complaint does not allege that LabMD engaged in any deceptive practices whatsoever. *See* Compl. ¶¶22-23.

PUBLIC

The FTC has not only repeatedly told Congress that the Commission does not have Section 5 jurisdiction over data-security practices but also repeatedly asked for the broad authority to regulate such practices. Congress, in turn, has repeatedly refused, delegating the FTC only very narrow and limited authority over data-security practices in circumstances that do not obtain here.[2] In fact, Congress has given the Department of Health and Human Services (HHS), and not the FTC, the sole and specific authority to regulate the patient-information data-security practices at issue in this case.

Even the President has rejected the FTC's power-grab approach to data-security regulation.[3] See Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

---

[2] Congress would not have made these specific delegations if it believed that the FTC had general Section 5 authority to regulate patient-information and other data-security practices. Rather, these delegations demonstrate that Congress ratified the Commission's historic understanding of the limits on its Section 5 jurisdiction and confirm that the FTC's Section 5 "unfairness" authority does not extend to the patient-information data-security practices at issue here. *See infra* Section I.B.

[3] The President apparently recognizes that the FTC's "sue now, offer guidance later" approach is bad policy and unconstitutional to boot. His Order requires the Department of Commerce, through the National Institute of Standards and Technology (NIST), to lead the creation of a baseline set of standards for a "Cybersecurity Framework" establishing a "set of standards, methodologies, procedures, and processes" and including implementation "guidance." *See* Exec. Order No. 13,636 § 7(b). The Framework must "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach" with specific "information security measures and controls" operators can implement to "identify, assess, and manage cyber risk." *Id.* NIST must "engage in an open public review and comment process." *Id.* § 7(d).

The FTC's attack on LabMD and other companies is contrary to each of the steps in the President's Executive Order for effective and lawful data-security regulation. The FTC has not (1) issued any standards, methodologies, procedures, or processes for Section 5 compliance; (2) established guidance for measuring implementation and performance of compliant data-security protections; (3) identified specific information security measures and controls that a business might adopt; or (4) engaged in an open public review and comment process. There is simply no reason why the FTC should not be required to follow the President's process of requiring rules, regulations, and standards *before* the government brings abusive enforcement actions and makes shifting and uncertain compliance demands.

PUBLIC

The Complaint is a classic example of regulatory overreach and, accordingly, it should be dismissed in its entirety with prejudice for the following reasons.

First, Congress has not given the FTC the power to use its Section 5 "unfairness" authority to do what it has done to LabMD here, and so this action is illegal and illegitimate. *La. Pub. Serv. Com. v. FCC*, 476 U.S. 355, 374 (1986).

Second, even if Section 5 authorized the FTC to broadly regulate data-security practices as "unfair" acts or practices, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as interpreted and enforced by HHS, control. More recent and more specific than the FTCA, HIPAA and HITECH manifest Congress's unambiguous intent to give HHS regulatory authority over patient-information data-security and to displace whatever Section 5 authority the FTC might have to regulate LabMD's data-security practices as "unfair" acts or practices.

Third, the FTC's failure to promulgate *any* data-security regulations, standards, or guidance that would allow LabMD to ascertain with reasonable certainty what data-security practices the Commission believes Section 5 to forbid or require, and its *ex post facto* enforcement practices, deny LabMD and others similarly situated of fair notice and violate the Constitution and the Administrative Procedure Act (APA).

Fourth, the acts or practices alleged in the Complaint are not "commerce" within the scope of the FTCA.

Fifth, the Complaint couches legal conclusions as factual statements and therefore fails to state a facially plausible claim for relief.

PUBLIC

STATEMENT OF FACTS

LabMD is a small medical company providing its physician-customers with cancer diagnoses. These physicians send LabMD their patients' blood, urine, and tissue for sampling, together with relevant patient identification and insurance information. LabMD does the testing and then sends back a diagnosis to the requesting doctor.

LabMD's patient-information data-security practices are, and were at all times relevant, regulated under HIPAA and HITECH. Congress tasked HHS to implement and enforce these statutes, and it has promulgated regulations to do so.[4] LabMD has never been accused of violating HIPAA or HITECH by the FTC, HHS, or anyone else. *See* Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 22:10-13 (Sept. 25, 2013)(hereinafter "Trans.").

The genesis of this action appears to have been in early 2008, when, without LabMD's knowledge or consent, Tiversa, Inc. (Tiversa), a government contractor that created and exploited data breaches to generate business, took possession of a single LabMD physician patient-information spreadsheet file (the "PI file"). Complaint, *Tiversa et al. v. LabMD et al.*, Dkt. 1, No. 2:13-cv-01296-NBF, at 4 ¶¶18-19 (W.D. Pa. Sept. 5, 2013)(hereinafter "Tiversa Compl."). Tiversa has boasted to Congress about its practice of taking computer files from unsuspecting third persons without their knowledge or permission using a "unique technology" unavailable to the general public. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa).

[4] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information" established and enforced by HHS); 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000)(HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013)(HHS's HITECH Breach Notification Rule).

PUBLIC

Tiversa said in a May 28, 2009, press release (since pulled from the Internet) that in "a typical day" it might see sensitive information "of tens of thousands" being unknowingly "disclosed" by a hospital or medical billing company, a third-party payroll provider, or a Fortune 500 company. *See* Press Release, "Tiversa Identifies Over 13 Million Breached Internet Files in the Past Twelve Months" (May 29, 2009). It also said that, working with Dartmouth College researchers under a government contract, it searched file-sharing networks for key terms associated with the top ten publicly traded healthcare firms in the country, and "discovered" what it called "a treasure trove of sensitive documents," such as a spreadsheet from an AIDS clinic with Social Security numbers, addresses, and birth-dates; hospital databases with Social Security numbers, contact details, insurance records, and diagnosis information on 20,000 patients; the PI file; and "350+ megabytes of data comprising sensitive reports relating to patients of a group of anesthesiologists."

After taking LabMD's property, Tiversa telephoned LabMD offering "remediation services" and a cost estimate. Tiversa Compl. ¶¶19-21. That same day, Tiversa sent LabMD three follow-up sales-pitch emails. *See LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842, 843 (11th Cir. 2013). Over the next two months, Tiversa sent six more sales-pitch emails to LabMD. *See id.* Communications between LabMD and Tiversa stopped only when "LabMD did not retain Tiversa's services." Tiversa Compl. ¶22.

Tiversa then gave the Commission the purloined PI file. Tiversa Compl. ¶¶25-26. Apparently, the PI file was the only file of those mentioned in Tiversa's Press Release given to the Commission. And, with this file in hand, the FTC began investigating LabMD. After years of intrusive and costly discovery, including multiple civil investigate demands (CIDs),

PUBLIC

depositions, and document productions, on August 28, 2013, the Commission voted unanimously to issue the Complaint.

The Complaint alleges that LabMD violated Section 5's prohibition of "unfair" acts or practices by allegedly engaging in data-security practices that, "taken together," fail to meet the Commission's unspecified standards. *See* Compl. ¶10. The Complaint does not allege that LabMD engaged in "deceptive" acts or practices. *Id*. ¶¶22-23. Nor does it allege that any "consumers" have suffered any harm due to the Tiversa take.[5] *Id*. ¶¶17-19. Instead, it alleges in vague, conclusory terms that LabMD engaged in unspecified "unfair acts or practices."

Tellingly, the Complaint does not cite any regulations, guidance, or other standards for what patient-information data-security practices the Commission believes to be "adequate" or "readily available" or "reasonably foreseeable" or "commonly known" or "relatively low cost." *Id*. ¶¶10-11. It does not specify what regulations, guidance, or standards LabMD fell short of or what combination of LabMD's alleged failures to meet these unspecified requirements, "taken together," violate Section 5. *Id*. ¶10. It does not allege that LabMD's claimed "security failures" caused "consumers" to suffer any economic or other injury. *See id*. ¶¶10-11, 17-21.

The Complaint alleges that LabMD's "Day Sheets and a small number of copied checks" were found by the Sacramento Police "in the possession of individuals who pleaded no contest to state charges of identity theft." *Id*. ¶21. But it does not allege that those "individuals" in fact used LabMD's Day Sheets and copied checks to engage in identity theft or caused any of LabMD's "consumers" to suffer any injury. *See id.* Instead, the Complaint alleges that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people

[5] As LabMD explained in its Answer, what the Complaint calls LabMD's "consumers" are in reality LabMD's referring physicians' patients. It is these physicians, and not their patients, who are LabMD's customers and the consumers of its diagnostic services.

PUBLIC

with different names"—which, even if true, may be mere correlation (the Complaint does not allege any causation)—and speculates that this "*may indicate* that the SSNs have been used by identity thieves." *Id.* (emphasis added).

Asked about other sources of data-security standards, the FTC said the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC pointed to "public statements made by the Commission" and so-called "educational materials that have been provided" as standards. Trans. 9:23-25. In addition, the FTC argued that "the IT industry…has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7. The FTC also referenced "guiding principles" and stated that "[t]here are lots of sources for the principles, such as materials published by the National Institute of Standards and Technology [NIST], continuing education for IT professionals, practical IT experience, and lessons learned from publicized breaches." Trans. 11:21-12:2.

But critically, the FTC did not claim that any of the above has the force of law or creates any binding duties and obligations.

The FTC also accused LabMD of violating Section 5 "by failing to provide reasonable security for sensitive information," opining "that reasonableness is a common sense balancing of cost and benefit and that common sense is available from many, many sources, including organizations—government organizations, such as the National Institute of Standards, private entities, such as the SANS Institute, and many others as well." Trans. 21:19-22:2. But again, the

PUBLIC

FTC did not claim that LabMD violated any data-security standards that have the force of law, such as the patient-information data-security regulations implementing HIPAA.

In fact, the FTC has not accused LabMD of violating any data-security statutes, rules, or regulations. At the initial pretrial conference, the ALJ asked: "Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?" Trans. 22:10-12. The FTC responded "No." Trans. 22:13. The FTC also admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17. The FTC has never promulgated patient-information data-security regulations, guidance, or standards under Section 5 and, apparently, it has no plans to do so: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act…for financial institutions." Trans. 10:11-15.

STANDARD OF REVIEW

A Respondent may raise jurisdictional and other legal defenses in a motion to dismiss, which is treated like a Fed. R. Civ. P. 12(b)(6) motion for failure to state a claim upon which relief can be granted. *In re Union Oil Co.*, 138 F.T.C. 1, 16 (F.T.C. 2004). The FTC bears the burden of establishing jurisdiction. *See* Commission Rule 3.43(a), 16 C.F.R. § 3.43(a); *In re POM Wonderful LLC*, 2012 FTC LEXIS 106, 463-65 (F.T.C. May 17, 2012)(Initial Decision). It may not do this by pleading legal conclusions, as it has done here. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Instead, there must be facts showing grounds for a plausible claim for relief, not merely labels and conclusions and a formulaic recitation of the elements. *Id. at 679; Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

PUBLIC

ARGUMENT

I. THE COMMISSION LACKS SECTION 5 "UNFAIRNESS" AUTHORITY TO REGULATE PATIENT-INFORMATION DATA-SECURITY PRACTICES.

Section 5 prohibits unfair acts or practices in or affecting commerce. 15 U.S.C. § 45(a)(1). The Commission does not have carte blanche to regulate anything and everything it unilaterally deems "unfair." *See, e.g., Scientific Mfg. Co. v. FTC*, 124 F.2d 640, 644 (3d Cir. 1941)(holding that Section 5 does not authorize the Commission to regulate publications "concerning an article of trade by a person not engaged or financially interested…in that trade," because otherwise it "would become the absolute arbiter of the truth of all printed matter"). In fact, in 1994 Congress enacted limiting language to control the FTC's misuse of its Section 5 unfairness authority. *See* 15 U.S.C. § 45(n); Howard Beales III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MKTG. 192 (2003)(former Director of FTC's Bureau of Consumer Protection describing how Congress "reigned in" Commission "abuse" of its Section 5 unfairness authority), *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 7, 2013).

The FTC must show that it has congressionally delegated authority to regulate LabMD's patient-information data-security practices. *City of Arlington v. FCC*, 133 S. Ct. 1863, 1869 (2013)(agencies' power to act and how they are to act is authoritatively prescribed by Congress, so when they act beyond their jurisdiction, what they do is ultra vires); *see, e.g., ABA v. FTC*, 430 F.3d 457, 468-71 (D.C. Cir. 2005)(holding that the FTC's interpretation of the Gramm-Leach-Bliley Act to authorize it to regulate attorneys engaged in the practice of law exceeded the Commission's statutory authority and was therefore invalid). And, the law requires the FTC to exercise its Section 5 unfairness authority consistent with the congressionally enacted administrative structure. *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125, 133

PUBLIC

(2000). Finally, the controlling authorities hold the scope of Section 5 authority must be viewed in the light of other relevant statutes, "particularly where Congress has spoken subsequently and more specifically to the topic at hand."[6] *Id.* at 133; *see also FTC v. Nat'l Cas. Co.*, 357 U.S. 560, 562-63 (1958), *superseded by statute* (examination of subsequent statute and its legislative history demonstrates that it limits the FTC's Section 5 regulatory authority).

Section 5's plain language does not authorize patient-information data-security regulation, and Congress has enacted many statutes that, taken together, independently prohibit the FTC from regulating patient-information data-security and strictly cabin its authority to regulate data-security practices in other economic sectors. The FTC does not have the authority to regulate LabMD's patient-information data-security practices. Therefore, the Complaint should be dismissed.

A. Congress Authorized HHS, Not The FTC, To Regulate Patient-Information Data-Security Practices.

Congress has enacted specific legislation, HIPAA and HITECH, setting patient-information data-security standards and delegating to HHS the relevant interpretative and enforcement authority. Consequently, even if Section 5 does authorize the FTC to regulate data-security, which it does not, the Commission lacks legal sanction for the things that it has done to LabMD.

1. Controlling interpretative canons hold the FTC's general Section 5 authority (if any) must yield to the specific patient-information statutes and regulations.

To begin with, the well-known interpretative canon that a general statute must yield to a more specific one applies here. As the Supreme Court recently held:

[6] The Commission has admitted to Congress that this is how Section 5 should be interpreted. *See* FTC, *Policy Statement on Unfairness* 2 (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

PUBLIC

> The general/specific canon...has full application as well to statutes such as the one here, in which a general authorization and a more limited, specific authorization exist side-by-side. There the canon avoids not contradiction but the superfluity of a specific provision that is swallowed by the general one, "violat[ing] the cardinal rule that, if possible, effect shall be given to every clause and part of a statute."

RadLAX Gateway Hotel, LLC v. Amalgamated Bank, 132 S. Ct. 2065, 2070-71 (2012)(citation omitted).

HIPAA requires LabMD to meet security standards for electronic health information, such as the PI file. HITECH requires HIPAA-regulated entities to provide notice of unsecured breaches of health information in certain circumstances and strengthens protections for such data. Congress vested HHS with exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws.[7] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information"). Recognizing this, the FTC has repeatedly told Congress that HIPAA and its privacy rule are not enforced by the Commission.[8]

---

[7] Unlike the Commission, HHS has actually promulgated regulations establishing reasonably ascertainable patient-information data-security standards.

[8] For example, in March 2005, Commission Chairwoman Deborah Majoras said that HIPAA is "not enforced by the Commission." *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Statement Before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs*, 109th Cong., 6 (2005). This understanding was reaffirmed before Congress in 2007. *See Protecting the Privacy of the Social Security Number from Identity Theft: Statement Before the Subcommittee on Social Security of the House Committee on Ways and Means*, 110th Cong. 10 (2007)(prepared statement of Joel Winston, FTC). The preambles to HHS's HIPAA rules refer to the single national standard the HIPAA regulations establish. *See* 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000)(Privacy Rule)("This…rule establishes, for the first time, a set of basic national privacy standards and fair information practices…."); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(Security Rule)("The purpose of this…rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information."); *see also* U.S. Dep't of Health & Human Servs., *Security 101 for Covered Entities, HIPAA Security Series*, Vol. 2/Paper 1, 3 (2007)("Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry."), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (accessed Nov. 3, 2013).

PUBLIC

HITECH's plain language confirms Congress's intent that data-security standards for HIPAA-covered entities be regulated exclusively by HHS, not the FTC. HITECH §13422(b)(1) directs HHS, in coordination with the FTC, to study data-security requirements for non-HIPAA-covered entities and determine "which Federal government agency is best equipped to enforce such requirements recommended to be applied to…[non-HIAPA-covered entities]…and a timeframe for implementing regulations based on such findings." Pub L. 111-5 § 13422(b)(1), 123 Stat. 226, 277 (2009); *see also* 42 U.S.C. § 17937 (giving the FTC authority to establish temporary data-breach notification requirements for non-HIPAA-covered entities).

If the Commission already had such authority, HITECH and many other data-security statutes would be superfluous. Indeed, if Congress intended to give the FTC authority to regulate patient-information data-security (or believed that the FTC already had this authority), then it would not have drawn a clear distinction between HIPAA-covered and non-HIPAA-covered entities and specifically given the FTC such limited authority to regulate non-covered entities, for the mention of one thing suggests the exclusion of another.[9] *See, e.g., United States v. Lopez*, 938 F.2d 1293, 1297 (D.C. Cir. 1991); *see Indep. Ins. Agents of Am., Inc. v. Hawke*, 211 F.3d 638, 645 (D.C. Cir. 2000)("[T]he cannons of avoiding surplusage and expressio unius are at their zenith when they apply in tandem."). Clearly, Congress charged HHS, and not the FTC, with regulating LabMD's patient-information data-security practices, and it is inappropriate for the Commission to bulldoze these boundaries. *See* 78 Fed. Reg. at 5,687-5,702.

[9]As HHS recently explained, the "entities operating as HIPAA covered entities and business associates are subject to HHS' and not the FTC's, breach notification rule." 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013); *accord* 74 Fed. Reg. 42,962, 42,964-65 (Aug. 25, 2009)("HIPAA-covered entities and entities that engage in activities as business associates of HIPAA-covered entities will be subject only to HHS' rule and not the FTC's rule….").

PUBLIC

2. The *Billing* doctrine controls and so the FTC has no authority.

Because there is a "clear repugnancy" between the specific and targeted regulatory enactments of HIPAA and HITECH, on the one hand, and Section 5's general unfairness language, on the other, the later must yield to the former, and so the FTC has no authority over LabMD's patient-information data-security. *See Credit Suisse Sec. LLC v. Billing*, 551 U.S. 264, 275 (2007).

In *Billing*, the Supreme Court held that the regulatory provisions of the securities laws, by implication, precluded the more general antitrust law. Preclusion obtained in that case based on an analysis of (1) the existence of regulatory authority under the securities law to supervise the activities in question; (2) evidence that the responsible regulatory entities exercise that authority; (3) a resulting risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct; and (4) the possible conflict between the laws with respect to affected practices that lie squarely within an area of financial market activity that the securities laws seek to regulate. *See id.* at 275-76.

HIPAA/HITECH and the FTC's claimed Section 5 authority to regulate patient-information data-security practices are "clearly incompatible," and so *Billing* holds that Section 5 and the FTC must yield. This is because (1) Congress gave HHS specific regulatory authority over patient-information data-security practices; (2) HHS exercises that authority, as evidenced by its repeated promulgation of data-security standards for healthcare providers, *see e.g.* 78 Fed. Reg. 5,566 (Jan. 25, 2013); (3) as demonstrated by this proceeding, there is a risk of conflicting standards of conduct (notably, the FTC agrees that LabMD has not violated HIPAA or HITECH, Trans. 22:10-13); and (4) this possible conflict with Section 5 affects practices that lie squarely within an area of healthcare activity regulated under HIPAA/HITECH. *See supra* notes 4 & 9.

PUBLIC

Thus, HIPAA/HITECH preclude application of Section 5 to LabMD's patient-information data-security practices. *See Billing*, 551 U.S. at 275-76.

B. Congress Has Not Given The FTC The Plenary Power To Regulate Data-Security Through Its Section 5 "Unfairness" Authority.

The FTC claims its general Section 5 "unfairness" authority allows it to regulate LabMD's patient-information data-security. However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope.

1. The FTC's claim of general Section 5 "unfairness" authority to regulate data-security practices is contradicted by Congress's many specific data-security delegations.

The FTC's claim of general Section 5 "unfairness" authority to regulate LabMD and other companies is contradicted by Congress's many specific delegations of data-security authority.

To begin with, when Congress has wanted the FTC to have data-security authority, it has said so. To date, Congress has specifically authorized the Commission to regulate data-security practices in at least three statutes, including the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA).[10] The FTC has argued elsewhere that the FCRA, GLBA, and COPPA merely "enhance FTC authority

[10] The FCRA, 15 U.S.C. § 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 111 Stat. 1952 (2003), establishes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies and requires the FTC and other agencies to develop rules for financial institutions to reduce the incidence of identity theft. The GLBA, Pub. L. 106-102, 113 Stat. 1338 (1999)(codified 15 U.S.C. §§ 6801-6809), mandates data-security requirements for financial institutions and instructs the FTC and federal banking agencies to establish standards for financial institutions "to protect against unauthorized access to or use of such records or information," 15 U.S.C. § 6801(b)(3). The COPPA, Pub. L. 105-277, 112 Stat. 2681 (1998)(codified 15 U.S.C. § 6501 *et seq.*), requires website operators to establish and maintain reasonable procedures to protect the confidentiality and security of information gathered from children.

PUBLIC

with new legal tools," such as "rulemaking and/or civil penalty authority…." Plaintiff's Opposition to Motion to Dismiss, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM, Dkt. No. 110, at 12 (D. N.J. May 20, 2013)(the "FTC Opposition"). But this argument fails, for these statutes explicitly authorize the Commission to set substantive data-security standards. *See* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and to enforce those standards under the FTCA, *see* 15 U.S.C. §§ 1681s(a), 6805(a)(7), 6505(d). If Section 5 generally authorized the FTC to do these things, these provisions would be meaningless exercises, *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 58 (2006), as "there would have been no reason for Congress to have included" them, *Stone v. INS*, 514 U.S. 386, 397 (1995). The Commission cannot assume that Congress passes purposeless legislation. *Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or.*, 515 U.S. 687, 701 (1995). Therefore, FCRA, GLBA, COPPA, and other narrowly tailored statutes are the only authorities authorizing the FTC to regulate data-security practices of any sort.

At the same time, Congress has enacted numerous other targeted statutes specifically delegating statutory authority over data-security, including HIPAA, HITECH, the Cable Television Consumer Protection and Competition Act, Pub. L. 102-385, 106 Stat. 1460 (1992)(codified at 47 U.S.C. § 521 *et seq.*); the Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 8195 (1988)(codified at 18 U.S.C. § 2710); Driver's Privacy Protection Act of 1994, Pub. L. 103-322, 106 Stat. 2099 (1994)(codified at18 U.S.C. § 123); and the Computer Fraud Abuse Act of 1986, Pub. L. 99-474, 100 Stat. 1213 (1986)(codified as amended at 18 U.S.C. § 1030 *et seq.*).[11] If the FTC's Section 5 unfairness authority included general, economy-wide authority to regulate data-security, then all of these statutes, creating and delegating regulatory

[11] This list is illustrative, not exhaustive.

PUBLIC

authority to HHS and other agencies, would also necessarily be superfluous nullities. The Commission's Section 5 power-grab here therefore offends the rule against attributing redundancy to Congress, *Gutierrez v. Ada*, 528 U.S. 250, 258 (2000), and is at odds with the interpretive canon that no statute should be interpreted in a fashion that renders its parts "inoperative or superfluous." *See Corley v. United States*, 556 U.S. 303, 314 (2009).

2. The Commission's claim of Section 5 "unfairness" authority to regulate data-security economy wide is contrary to congressional intent and to controlling Supreme Court authorities.

As the Commission itself frequently acknowledged—until it recently reversed course without explanation or opportunity for notice and comment from stakeholders, both in violation of the law, *see FCC v. Fox TV Stations, Inc.*, 556 U.S. 502, 514-15 (2009)(an agency must explain policy change)—Section 5 does not give the FTC the authority to regulate data-security practices as "unfair" acts or practices or the authority to require firms to adopt information practice policies.[12] This is why Congress enacted FCRA, GLBA, COPPA, HIPAA, HITECH, and numerous other targeted data-security laws.

[12] For many years, the Commission said its authority over data-security matters was "limited...to ensuring that Web sites follow their stated information practices." *Consumer Privacy on the World Wide Web, Hearing before Subcomm. on Telecomm. of the H. Comm. on Commerce Subcomm. on Telecomm.*, 105th Cong. n.23 (1998)(statement of Robert Pitofsky, Chairman, FTC), *available at* http://www.ftc.gov/os/1998/07/privac98.htm; *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 137 (2008). As a Commission official explained in 2001, "'[t]he agency's jurisdiction is (over) deception….The agency doesn't have the jurisdiction to enforce privacy.'" Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired (May 31, 2001), http://www.wired.com/politics/security/news/2001/05/44173 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC); *accord* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 34 (2000)(hereinafter "*2000 Privacy Report*"), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (accessed November 3, 2013); FTC, *Privacy Online: A Report to Congress*, 41 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf ("Commission [generally] lacks authority to require firms to adopt information practice policies….")(accessed Nov. 3, 2013); *see also Protecting Information Security and Preventing Identity Theft, Hearing before Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of H. Comm. on Gov't Reform,*

PUBLIC

The Commission's lack of power to regulate data security through its general Section 5 "unfairness" authority also explains why the Commission has, for over a decade, asked Congress for legislation authorizing it to do what it has done to LabMD.[13] In May 2012, John Leibowitz, then-Commission Chairman, asked once more for the power to enforce data-security measures.[14] Yet, Congress has consistently refused, over a period of many years, to give the Commission what it wants,[15] considering and rejecting several proposals to give the

---

108th Cong. 7 (statement of Orson Swindle)(2004)("To date, the Commission's security cases have been based on its authority to prevent deceptive practices."), *available at* http://www.ftc.gov/os/2004/09/040922infosecidthefttest.pdf (accessed Nov. 3, 2013).

[13] *See, e.g.*, *2000 Privacy Report* at 36-37 (asking Congress to enact legislation requiring websites to "take reasonable steps to protect the security of the information they collect" and providing "the authority to promulgate more detailed standards"); *see also Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of David C. Vladeck, Director of the Bureau of Consumer Protection, FTC)("[T]he Commission reiterates its support for federal legislation that would…impose data security standards on companies…."); *Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of Edith Ramirez, Commissioner, FTC)(same); *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before H. Comm. on Energy & Commerce*, 111th Cong. 12 (2009)(prepared statement of Eileen Harrington, FTC)(The FTC "has recommended legislation requiring all companies that hold sensitive consumer data to take reasonable measures to safeguard it.").

[14] *Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing Before S. Comm. on Commerce, Science, and Transportation* 112th Cong. 1-2 (2012)(statement of John Leibowitz, Chairman, FTC). Leibowitz noted in a footnote that then-Commissioner Thomas Rosch believed that "in contravention of our promises to Congress, [the Commission's] privacy framework is based on an improper reading of our consumer protection 'unfairness' doctrine…." *Id.* at 3 n.2. Indeed, even the Commission's 2008 Resolution did not claim that the Commission can regulate data-security practices under a pure unfairness theory. *See* Resolution Directing Use of Compulsory Process In Nonpublic Investigation of Acts and Practices Related to Consumer Privacy And/Or Data Security, File No. P954807 (Jan. 3, 2008)(authorizing an investigation into "deceptive or unfair acts or practices related to consumer privacy and/or data security…in violation of Section 5"). The Complaint has not alleged that LabMD engaged in deceptive practices. *See* Compl. ¶¶22-23.

[15] *See, e.g.*, Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Breach Notification Act of 2011, S.1408, 112th Cong. (2011); Data Security Act of 2011, S.1434, 112th Cong. (2011); Personal Data Protection and Breach Accountability Act of 2011,

PUBLIC

Commission the general authority to regulate data security. *Cf. Brown & Williamson*, 529 U.S. at 147. In other words, Congress has ratified the Commission's previous position that it lacks general jurisdiction to regulate data-security practices under Section 5.[16] *See id.* at 156.

If Congress had intended for the Commission's Section 5 "unfairness" authority to include patient-information data-security practices, it could have said so in the Federal Trade Commission Act Amendments of 1994, codified at 15 U.S.C. § 45(n). Instead, due to a long history of Commission abuses, Congress stripped it of the authority "to declare unlawful an act or practice" under Section 5 unless "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.*; *see* Statement by Director of Consumer Protection Howard Beales, *FTC's Use of Unfairness Authority*, *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 3, 2013). Congress also said that public policy concerns are not a primary basis for the exercise of jurisdiction, 15 U.S.C. § 45(n), thereby legislatively overruling prior judicial Section 5 interpretations. *See, e.g.*, *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 369 (1965), *superseded by statute.*

At the time, the Commission did not claim Section 5 "unfairness" authority to regulate patient-information (or any other) data-security practices. But now it has changed its tune and

---

S. 1535, 112th Cong. (2011); Data Accountability and Trust Act, H.R 1707, 112th Cong. (2011); Data Accountability and Trust Act of 2011, H.R 1841, 112th Cong. (2011); SAFE Data Act, H.R. 2577, 112th Cong. (2011).

[16] The Commission's extralegal approach to data-security regulation also violates the core principles espoused in Executive Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013), which directs the Department of Commerce (not the Commission) to identify specific data-security practices through the notice-and-comment process, *see id.* § 7; *see also* Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at 29 n.33 (Feb. 2012)("[T]he FTC does not currently have authority to enforce Section 5…against certain corporations that operate for profit…."), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

PUBLIC

grabs for massive plenary powers over the entire economy. Yet, Section 5 does not and was not intended to give the Commission authority to do this. Congress does not hide massive regulatory schemes in statutory mouseholes. *Whitman v. Am. Trucking Ass'ns., Inc.*, 531 U.S. 457, 468 (2001); *see also Brown & Williamson*, 529 U.S. at 160. This holds true *a fortiori* where, as here, the Commission claims its broad authority from vague general statutory terms in the face of both an amended Section 5 that was designed to rein in the Commission's abuse of its "unfairness" authority and a raft of specific, targeted data-security statutes, including HIPAA and HITECH.

Simple "common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude," *Brown & Williamson*, 529 U.S. at 133, as general regulatory authority over the data-security practices of all private businesses in the United States reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint. As in *Brown & Williamson*, to conclude that Section 5 gives the FTC jurisdiction over data-security requires not only an "extremely strained understanding" of a vague term ("unfairness") in the FTCA, *cf. id.* at 160-61 (discussing FDA's misinterpretation of the word "safety" in the Food, Drug, and Cosmetic Act), "but also ignor[ing] the plain implication of Congress' subsequent…[data-security]-specific legislation," *id.* at 160. There, as here, Congress could not have intended to grant unfettered power to prescribe data-security standards for private companies, a topic of intense debate with immense economic consequences, to the Commission "in so cryptic a fashion." *Id.* at 160.

In *Brown & Williamson* the Supreme Court rejected the FDA's overreaching. *See id.* at 125. There, as here, the agency pestered Congress to pass legislation expanding its authority but Congress instead chose a more targeted, narrowly tailored regulatory scheme. *See id*. at 153-

PUBLIC

54, 156, 158 (Congress enacted numerous tobacco-specific statutes incrementally expanding regulatory authority). Thus, *Brown & Williamson* controls and requires rejection of the Commission's claimed Section 5 "unfairness" authority to regulate LabMD's patient-information data-security practices.

C. *ABA v. FTC* Stands For Dismissal.

The case of *ABA v. FTC*, 430 F.3d at 470-71, stands for dismissal.

There, the D.C. Circuit denied the FTC's attempted power-grab to regulate attorneys under the GLBA, ruling that Congress had not directly and plainly granted the Commission the authority to regulate and rejecting the FTC's claim that statutory gap-filling justified a massive expansion of its authority. *See id.* at 470-71. The court said that Congress's decision not to specifically authorize attorney regulation in the GLBA "makes an exceptionally poor fit with the FTC's apparent decision that Congress, after centuries of not doing so, has suddenly decided to regulate the practice of law." *Id*. at 470. It also said that attorney regulation was historically the province of the states and that federal law "'may not be interpreted to reach into areas of State sovereignty unless the language of the federal law compels the intrusion.'" *Id.* at 472 (citation omitted).

ABA's reasoning applies with equal force here. First, there is nothing in Section 5 explicitly authorizing the FTC to directly regulate patient-information data-security practices. Instead, as in *ABA*, the Commission is simply grabbing power to "fill in" what it perceives to be a regulatory gap. But Congress has already filled the patient-information data-security regulatory "gap" through HIPAA and HITECH, and it is not for the FTC to second-guess Congress. The FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See id.* at 470-71; *see also Brown & Williamson*, 529 U.S. at 160.

PUBLIC

Second, Congress has generally left healthcare-provider data-security regulation to the states. This is because regulation of privacy and healthcare is traditionally a matter of local concern.[17] *See* 65 Fed. Reg. at 82,463 ("Rules requiring the protection of health privacy in the United States have been enacted primarily by the states."); *see also Hill v. Colo.*, 530 U.S. 703, 715-18 (2000)(upholding statute protecting patient privacy as valid exercise of state's traditional police power to protect health and public safety); *Hillsborough Cnty. v. Automated Med. Laboratories*, Inc., 471 U.S. 707, 719 (1985)(The "regulation of health and safety matters is primarily, and historically, a matter of local concern."). In those cases where Congress has determined federal regulation of patient-information data-security practices is appropriate, it has explicitly said so. *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1). Because Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's intrusion into patient-information data-security, its brazen fabrication of authority and grab for power should be rebuffed. *See ABA*, 430 F.3d at 472.

[17] Pub. L. No. 104-191, 110 Stat. 1936, § 264(c)(2) states that HIPAA regulations "shall not supersede a [more robust] contrary provision of State law," consistent with traditional state regulation of public health and welfare. *See Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996); *see also* John R. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, J. HEALTH & LIFE SCI. L., January 2008, at 1, 1 ("Before HIPAA, state privacy and confidentiality laws were almost the exclusive source of information protection requirements. HIPAA still defers to state laws that are more protective of PHI…."); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies And Laws*, 19 ALB. L. J. SCI. & TECH. 91, 104-105 & n.66 (2009)(noting that "all but six states and the District of Columbia have passed legislation requiring entities, particularly businesses that maintain computerized personal information…, to notify those residents if their personal information has been disclosed through a data breach" and listing statutes).

PUBLIC

II. THE COMMISSION HAS FAILED TO GIVE FAIR NOTICE OF WHAT DATA-SECURITY PRACTICES IT BELIEVES SECTION 5 FORBIDS OR REQUIRES THEREBY VIOLATING LABMD'S DUE PROCESS RIGHTS.

The Commission has refused to publish data-security regulations, guidance, or standards explaining what is either forbidden or required by Section 5. Therefore, it has denied LabMD and others similarly situated constitutionally required fair notice, engaged in prohibited *ex post facto* enforcement, and, through this action, violated LabMD's due process rights. *See Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)(traditional concepts of due process incorporated into administrative law preclude agencies from penalizing private parties for violating rules without first providing adequate notice of their substance); *Trinity Broad. of Fla., Inc. v. FCC*, 211 F.3d 618, 632 (D.C. Cir. 2000)(where the regulations and other policy statements are unclear, where the petitioner's interpretation is reasonable, and where the agency itself struggles to provide a definitive reading of the regulatory requirements, a regulated party is not "on notice" and may not be punished).

A. Due Process Requires Fair *Ex Ante* Warning of Prohibited or Required Conduct.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). Administrative law has thoroughly incorporated this constitutional fair notice requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *See Satellite Broad. Co. v. FCC*, 824 F.2d at 3. Where, as here, a party first receives notice of a purportedly proscribed activity through an enforcement action, due process rights are violated. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1355 (D.C. Cir. 1998)(due process requires fair notice of standard before company could be ordered to recall vehicles for alleged noncompliance with standard).

PUBLIC

B. The Commission Has Denied LabMD Fair Notice.

The test for constitutionally adequate notice is whether by reviewing the regulations and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards to which the agency expects parties to conform. *Trinity Broad.*, 211 F.3d at 632. The Commission "has the responsibility to state with ascertainable certainty" what standards third parties must follow. *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986)(citation omitted). It has failed to do so in this case.

The Commission is authorized to prescribe regulations specifically defining unfair acts or practices. 15 U.S.C. § 57a(a)(1). However, Section 5 independently bars the Commission from attempting to enforce consent orders against non-parties. 15 U.S.C. § 45(m)(1)(B). And the APA categorically prohibits federal agencies from creating legislative rules and substantive standards through mechanisms other than formal or notice-and-comment rulemaking. Consequently, the Commission cannot point to any legally-binding data-security standards, and so its attack against LabMD violates the company's due process rights.

1. The Commission has wrongfully failed to provide *ex ante* notice through regulations.

Section 5's general prohibition of "unfair" acts or practices is constitutionally too vague to provide adequate *ex ante* notice of the patient-information data-security practices that it purports to forbid or require. *See Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)(statute that either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates due process); *Trinity Broad.*, 211 F.3d at 632. Furthermore, the FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law. Trans. 21:11-22:13.

PUBLIC

The FTC's refusal to issue regulations is wrongful and makes no sense. It has in the past issued data-security regulations after notice-and-comment rulemaking in a number of areas. For example, 16 C.F.R. Pt. 314 sets forth specific standards under the GLBA "for developing, implementing, and maintaining reasonable" technical safeguards to protect consumer information. *See* 16 C.F.R. § 314.1. Also, 16 C.F.R. Pt. 682 implements the FCRA by articulating specific guidelines regarding the proper destruction of consumer information. *See* 16 C.F.R. § 682.3. Therefore, there is no reason the FTC could not have announced similar *ex ante* rules here, other than the FTC's admission that it prefers the "regulatory flexibility" of employing a vague standard such as "reasonableness." *See* FTC Opposition at 21-22; Trans. 21:11-25. But unchecked discretion is not a virtue of the FTC's current interpretation of its Section 5 "unfairness" authority, and it is for that very reason that such a regime cannot be lawful. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999)(boundless enforcement discretion violates due process); *Connally*, 269 U.S. at 391.

2. <u>The FTC's alleged "standards" are legally meaningless.</u>

The FTC has claimed that its "public statements," "educational materials," and "industry guidance pieces" establish standards and provide LabMD and others similarly situated with notice of the data-security practices they must keep to avoid Section 5 "unfairness" liability. Trans. 9:23-10:3. This claim is untenable for several reasons.

First, general statements of policy are prospective and do not create obligations enforceable against third parties like LabMD. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a…policy statement announces the agency's tentative intentions for the future." (citation omitted)); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006)(in holding agency manuals to be nonbinding, the court said that "it is particularly noteworthy that

PUBLIC

NPS did not issue its management policies through notice and comment rulemaking under 5 U.S.C. § 553" because failure to do so is evidence that the material in question was not supposed to be a rule binding regulated companies' conduct).

Second, if the FTC truly considers "public statements," "educational materials," and "industry guidance pieces" to be enforceable standards, then it necessarily concedes an APA violation. The APA requires agencies to "publish in the Federal Register for the guidance of the public…substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D). It further provides that except to the extent "that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published." 5 U.S.C. § 552(a)(1).

Therefore, the Internet postings of "Guides for Business," links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication.[18] The D.C. Circuit has never found that Internet notice is an acceptable substitute for publication in the Federal Register, and has affirmatively refused to do so. *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001). Here, the Complaint does not even allege that LabMD had actual notice of any of these sources. Thus, the FTC has breached its statutory duty.[19]

---

[18] Curiously, other Commission "business guides" that have been posted on the Internet have also been published in the Federal Register. *See, e.g.*, Guides for Jewelry, Precious Metals, and Pewter Industries, 16 C.F.R. § 23 (2013), *available at* http://www.ftc.gov/os/2012/06/120622jewelryguidesfrn.pdf.

[19] The FTC claims that NIST publications allegedly setting forth "principles" about what they call the "general approach" of "[d]efense in depth," Trans. 11:18-24, establish ascertainable standards. That claim is contradicted by NIST itself. A NIST publication

PUBLIC

Third, the FTC cannot regulate by consent order. *See Gen. Elec. Co. v. EPA*, 290 F.3d 377, 382-83 (D.C. Cir. 2002)(holding that an agency guidance document that imposes binding duties and obligations violates the APA). Consent orders "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement," *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). They do not restrict the FTC's discretion in future actions and therefore do not provide the fair notice that due process requires. *See Morales*, 527 U.S. at 63-64.

Furthermore, Congress specifically barred the Commission from binding third parties by consent order, prohibiting the FTC from enforcing a "consent order" against anyone who is not a party to it.[20] 15 U.S.C. § 45(m)(2); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir.

---

addressing the HIPAA Security Rule states: "This publication is intended as general guidance only…*and is not intended to be, nor should it be construed or relied upon as legal advice or guidance to nonfederal entities or persons*. This document does not modify…[]HIPAA[] or any other federal law or regulation." Scholl et al., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Pub. 800-66 Revision 1, at iv (2008)(emphasis added). Another NIST publication regarding computer security that the FTC may cite specifically disclaims any intent to establish standards: "*The purpose of this handbook is not to specify requirements*…." *An Introduction to Computer Security: The NIST Handbook*, NIST Special Pub. 800-12, at 3 (1995)(emphasis added). That argument therefore fails.

The FTC also argues that the SANS Institute establishes data-security standards that LabMD should have complied with. That, too, is wrong. The SANS Institute is merely a "cooperative research and education organization." SANS, About, http://www.sans.org/about/. It does not have the authority to prescribe legislative rules or otherwise establish binding standards. Voluntary industry standards are not law and do not purport to reveal what the Commission (or any other entity) believes Section 5 to require. *See, e.g., Romero v. Buhimschi*, 2007 U.S. Dist. LEXIS 73024, at *11 (E.D. Mich. 2007)(illustrating proposition that voluntary adoption of private standards of conduct does not create legal duty). Private standards cannot provide the fair notice the Commission has refused to give.

[20] The FTC may assert that consent orders in *other* data-security cases establish reasonably ascertainable standards. *See* FTC Opposition at 19. But, as the Commission has admitted, *see id.*, its prior consent orders are not "controlling precedent for later Commission action" and do not in any way limit the Commission's enforcement powers. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976). Even if Commission consent orders involving data-security practices could provide notice, which they cannot, Commission consent orders made

2007)(The FTCA "specifically provides that the Commission cannot enforce them against non-parties.").

Finally, none of the alleged standards cited by the FTC, whether NIST and SANS Institute publications, the Commission's patchwork-quilt of nonbinding consent orders (most of which, unlike this matter, involved allegations of deception), or general "Guides for Businesses" and "Consumer Alerts" purport to establish specific patient-information data-security standards that businesses "shall" or "must" abide by. Instead, these alleged sources of data-security standards are couched in, at best, precatory language: "may," "best practices," "recommendations," and the like.[21]

---

publicly available for the first time years after LabMD's alleged "security incidents" cannot give LabMD constitutionally adequate *ex ante* warning. *See, e.g.*, FTC, EPN, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,387 (June 13, 2012); FTC, Franklin Budget Car Sales, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,391 (June 13, 2012).

[21] The FTC may dismiss LabMD's arguments by claiming, as the Commission has elsewhere, that "[LabMD] may argue that it did not know *which* standard it was supposed to follow. This argument misses the point." FTC Opposition at 18 n.5 (emphasis in original). But that is one of LabMD's core points, for "baffling and inconsistent" rules do not give fair notice. *Satellite Broad.*, 824 F.2d at 2-4. Also, the FTC may argue that its Internet postings such as "Protecting Personal Information: A Guide for Business (2007), http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf (hereinafter "PPI Guide"), are enough. *See* FTC Opposition at 18-19. But this "Guide for Business" states that "there's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers." PPI Guide at 23. This is hardly "fair notice" of anything at all.

In 2011, the Commission also posted on the Internet a document entitled "Peer-to-Peer File Sharing: A Guide for Business." But the Complaint's allegations regarding a "P2P file sharing application" occurred in 2008, three years *before* this document was posted on the Internet. Moreover, it does not cite Section 5 or *any* regulations or binding standards. It does not make clear what, if anything, businesses are legally required or prohibited from doing, e.g., "[w]hether you decide to ban P2P file sharing programs on your network or allow them, it's important to create a policy and take the appropriate steps to implement and enforce it…." FTC, *Peer-to-Peer File Sharing: A Guide for Business* 3 (2011), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.pdf. Simply put, this document contains nothing resembling an intelligible, much less enforceable, binding legal standard.

PUBLIC

Consequently, the FTC has denied LabMD and others similarly situated the fair notice they are entitled to as a matter of constitutional right. *Gates & Fox Co.*, 790 F.2d at 156.

III. THE ACTS OR PRACTICES ALLEGED IN THE COMPLAINT DO NOT AFFECT INTERSTATE COMMERCE.

FTCA Section 4 defines "commerce" as commerce "among" or "between" states. 15 U.S.C. § 44; *see FTC v. Buntes Bros., Inc.*, 312 U.S. 349, 351-55 (1941). Section 5 allows the Commission to regulate "unfair…acts or practices in or affecting commerce" that have actually caused substantial (usually monetary) harm. 15 U.S.C. § 45(a)(1); *In the Matter of Int'l Harvester,* 104 F.T.C. 949, at 248 (1984)(unfairness cases usually involve "actual and completed harms," often monetary but sometimes health and safety). LabMD's principal place of business, where all of the alleged acts or practices allegedly occurred, is located in Georgia. Compl. ¶1. All of its servers and its computer network are located in Georgia. None of the alleged FTCA violations allegedly occurred outside of Georgia and there are no allegations of monetary loss or other actual harm. Therefore, dismissal with prejudice is appropriate.

IV. THE COMPLAINT DOES NOT COMPLY WITH THE COMMISSION'S PLEADING REQUIREMENTS.

Although the Commission's "unfairness" claim hinges on proving that LabMD's data-security practices were not "industry standard" or "commercially reasonable," the Complaint contains no allegations at all explaining what data-security practices were "standard" in the medical industry between 2008 and 2012, when the alleged "Security Incidents" occurred, or how LabMD's practices fell short of this unspecified benchmark. Further, the addition of technical jargon surrounding the Commission's claim of unreasonableness does not change that the Complaint's allegations are nothing more than inadequate "legal conclusion[s] couched as…factual allegation[s]." *Twombly*, 550 U.S. at 555 (citation omitted).

PUBLIC

The FTC does not dispute that LabMD complied with HIPAA and HITECH. Trans. 22:10-13. Moreover, the Complaint fails to allege any actual, completed economic harms or threats to health or safety. Therefore, the Complaint does not state a plausible claim for relief and should thus be dismissed.

V. THIS MATTER SHOULD BE STAYED PENDING DISPOSITION OF THIS MOTION.

Under its Rules of Practice, the Commission has the discretion to stay this matter pending its resolution of this Motion. Rule 3.22(b), 16 C.F.R. § 3.22(b)(Commission authorized to stay proceedings); Rule 3.21(c)(1), 16 C.F.R. § 3.21(c)(1)(Commission may continue evidentiary hearing for good cause); Rule 3.41(b), 16 C.F.R. § 3.41(b)(same). The Commission should exercise its discretion here and grant LabMD's request for a stay pending the resolution of its Motion to Dismiss.

In support of its action against LabMD, the FTC has undertaken extensive and abusive discovery. Notwithstanding years of investigation, multiple CIDs, depositions of LabMD's principals, and the production of thousands of pages of documents, the FTC has served burdensome, repetitive, and oppressive discovery requests that would not be allowed under the Federal Rules of Civil Procedure. For example, in a three-hour period on October 24, 2013, the FTC noticed twenty (20) depositions to be taken in various parts of the country, all of which were initially scheduled at the same time on the same day;[22] served eleven (11) subpoenas duces tecum; and served the FTC's First Set of Requests for Production and Interrogatories.

[22] In recognition of the burden and expense of depositions for private litigants that, unlike large federal agencies, do not have unlimited resources, in federal court, leave of court is (quite sensibly) required if a party wishes to take more than ten depositions. Fed. R. Civ. P. 30(a)(2)(A)(i). For that matter, Complaint Counsel has already deposed one of the named deponents during its investigation of LabMD. In federal court, leave of court would also be required for this, for obvious reasons. Fed. R. Civ. P. 30(a)(2)(A)(ii).

PUBLIC

LabMD has moved for a protective order. However, it is clear that the FTC's intentions include the punishment of LabMD and subjecting it to ruinous litigation costs, perhaps to chill others from contesting Commission overreach,[23] and all at taxpayer expense. Forcing LabMD to litigate a case that the Commission does not even have jurisdiction to bring is inherently unjust and violates its due process rights. Therefore, a stay of the administrative proceedings until LabMD's Motion to Dismiss is finally resolved would be appropriate.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion to Dismiss and ORDER that the Complaint be dismissed with prejudice. LabMD further requests that the Commission GRANT its Motion for a Stay of Administrative Proceedings pending the disposition of its Motion to Dismiss.

[23] Notably, the Complaint (along with a FTC press release making disparaging claims about LabMD) was issued shortly before publication of LabMD's CEO's book, *The Devil Inside the Beltway*, in which he exercises his First Amendment right to speak candidly about a matter of public concern and criticizes Complaint Counsels' actions and the Commission's treatment of LabMD in great detail. Complaint Counsels' burdensome and oppressive discovery requests—which run afoul of norms of conduct that obtain in Article III courts and *flagrantly* violate Fed. R. Civ. P. 30(a)(2)(A)'s limits on depositions—followed shortly after the book's publication. The First Amendment prohibits government agencies from retaliating against private citizens for engaging in constitutionally protected speech by bringing baseless enforcement actions. *See Trudeau v. FTC*, 456 F.3d 178, 190-91 nn.22-23 (D.C. Cir. 2006).

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: November 12, 2013

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	

[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE

This matter came before the Commission on November 12, 2013, upon a Motion to Dismiss the Complaint with Prejudice ("Motion") filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rule 3.22(a), 16 C.F.R. §3.22(a), for an Order dismissing the Federal Trade Commission's ("FTC") Complaint with prejudice. Having considered LabMD's Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that the FTC's Complaint is DISMISSED with prejudice.

ORDERED:

_____
Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Commissioners

Date:

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: November 12, 2013

By: _____
Michael D. Pepson

EXHIBIT 27

ORIGINAL

PUBLIC

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
APR 21 2014
569557
SECRETARY

COMMISSIONERS: Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	DOCKET NO. 9357
	)	
	)	PUBLIC
LabMD, Inc.,	)	
a corporation.	)	ORAL ARGUMENT REQUESTED

RESPONDENT LabMD, INC.'S MOTION FOR SUMMARY DECISION

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9100
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and proceedings before federal agencies.

Counsel for Respondent LabMD, Inc.

PUBLIC

TABLE OF CONTENTS

INTRODUCTION 3

STATEMENT OF FACTS 4

STANDARD OF REVIEW 8

ARGUMENT 9

I. SECTION 5's UNFAIRNESS PROVISION DOES NOT AUTHORIZE FTC TO CREATE A COMMON LAW OF PHI DATA SECURITY 9

II. THE FTC HAS FAILED THE FAIR NOTICE TEST AND VIOLATED DUE PROCESS. 11

III. IF FTC MAY OVER-REGULATE HIPAA, IT MAY OVER-REGULATE ALL OTHER REGULATED AREAS AFFECTING CONSUMERS. 18

IV. EVEN IF FTC PROVIDED LABMD FAIR NOTICE, HIPAA CONTROLS. 19

CONCLUSION 22

PUBLIC

RESPONDENT LabMD, INC'S MOTION FOR SUMMARY DECISION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

Please take notice that, pursuant to Commissions Rules 3.22 and 3.24, 16 C.F.R. §§ 3.22 and 3.24, Respondent LabMD, Inc., hereby moves for summary decision in its favor, and requests that the Administrative Complaint be dismissed in its entirety with prejudice.

INTRODUCTION

LabMD, Inc. ("LabMD") is being singled out by the Federal Trade Commission ("FTC") for its allegedly deficient data-security practices. All information received, utilized, maintained and transmitted by LabMD is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *See* 45 C.F.R. § 160.103. The FTC takes the position that it has Section 5 unfairness authority to create and enforce opaque "common law" regulations governing PHI data-security. Currently, the FTC's opaque "common law" regulations consist of negotiations, consent decrees, public statements made by the Commission, educational materials and internet posts which when taken together create additional and far more stringent and inconsistent standards than those promulgated by the Department of Health and Human Services ("HHS").[1] Even if FTC has such authority, it has failed to provide the constitutionally required fair notice of the PHI data-security standards that it seeks to enforce.

After more than four years of thorough investigation and litigation, including the depositions of FTC's Rule 3.33 designee and expert witnesses, FTC continues to take the position that it is not constitutionally required to specify in advance of investigation and

[1] HHS was granted Congressional rulemaking authority and promulgated regulations governing PHI data security standards through transparent, public notice and comment rulemaking.

PUBLIC

litigation the FTC data-security standards applicable to LabMD or similarly situated HIPAA "Covered Entities." *See* 45 C.F.R. § 160.103.

STATEMENT OF FACTS

The following facts are undisputed:

LabMD is a small, privately-owned medical laboratory providing cancer diagnoses through blood, urine, and tissue sample testing. Its customers are physicians. The physicians send their samples to LabMD, together with the relevant patient identification and insurance information, and LabMD sends back to the physicians the relevant diagnosis.

LabMD is a "Covered Entity" that receives, maintains and transmits PHI during the normal course of its business. *See* 45 C.F.R. § 160.103.

On or about February 5, 2008, without LabMD's knowledge or consent, Tiversa, Inc. ("Tiversa"), took possession of a single LabMD insurance aging file (the "Insurance Aging File"). Deposition of Robert Boback, dated Nov. 21, 2013, at 25, attached hereto as Exh. 1.[2]

The Insurance Aging File contained PHI for over 9,000 patients of LabMD's physician clients.

Subsequently, Tiversa made the Insurance Aging File available to Professor Eric Johnson, of Dartmouth College, who was conducting research under a government contract for his article entitled, "Data Hemorrhages in the Health Care Sector". *See* Data Hemorrhages in the Health-Care Sector at 1 fn. 1, attached in relevant part hereto as Exh. 2.

In January 2010, the FTC began a three year full investigation of LabMD's data security practices based upon the disclosure of the PHI contained in the Insurance Aging File.

[2] Tiversa has testified before Congress that it possesses unique technology which among other things allows it to download computer files from unsuspecting third persons inadvertently sharing computer files via peer to peer ("P2P") networks. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa, Inc.).

PUBLIC

In October 2012, during a raid of a house of suspected identity thieves, the Sacramento Police Department found LabMD "day sheets" and copies of checks made payable to LabMD. Again, the day sheets and checks contained PHI from patients of LabMD's physician clients. Deposition of Detective Jestes, dated Dec. 17, 2013, at 29-30, 33-36, attached hereto as Exh. 3.

In an attempt to notify LabMD of its find, the Sacramento police "googled" LabMD, and discovered that LabMD was under investigation by the FTC. Deposition of Detective Jestes, dated Dec. 17, 2013, at 27-28, 56, attached hereto as Exh. 3.

The Sacramento police then notified the FTC of its find, but did not notify LabMD, despite Sacramento's awareness of LabMD's duty to notify under HIPAA. Deposition of Detective Jestes, dated Dec. 17, 2013, at 28, attached hereto as Exh. 3.

In August, 2013, FTC filed an Administrative Complaint. *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("Compl.") (Aug. 28, 2013).

LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Opp'n") (Nov. 22, 2013) at 22 fn 15. It must comply with HHS's HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations, including HHS's HIPAA Privacy Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000); HHS's HIPAA Security Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003); and HHS's HITECH Breach Notification Rule, 78 Fed. Reg. 5,566 (Jan. 25, 2013).

HIPAA's Security Rule establishes substantive data-security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply.

HHS exclusively enforces HIPAA and HITECH. Order on Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Order")(Jan. 16, 2014), at 12 & n.19

PUBLIC

("[T]he Commission cannot enforce HIPAA and does not seek to do so. ... The Commission does not enforce HIPAA or HITECH....").

The FTC has not accused LabMD of violating HIPAA, HITECH or any implementing regulations. Compl. ¶¶ 22-23; Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, 22:10-13 (Sept. 25, 2013) ("Trans."); MTD Order at 12 n. 20 (Jan. 16, 2014); Complaint Counsel's Resp. to LabMD's RFAs, ("CC's RFA Responses") at 8-9 ¶¶ 7-8, attached hereto as Exh. 4.

The FTC alleges that LabMD's data-security is inadequate to protect the PHI it possesses and that this failure to adequately protect PHI is an unfair practice affecting consumers in violation of Section 5 of the Federal Trade Commission Act.

The FTC's expert opines that these failures persisted from January 2005 through July 2010 ("the relevant time period"). *See* Complaint Counsel's Expert Report of Professor Raquel Hill at 1, attached hereto as Exh. 5.

The FTC has never specified what data security standards were in place at any given point during the relevant time period or when LabMD specifically violated them.

The FTC claims it need not "allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use." CC's RFA Responses at 6-7 ¶ 5, attached hereto as Exh. 4.

When asked by the ALJ whether "the Commission issued guidelines for companies to utilize to protect...[sensitive] information or is there something out there for a company to look to," the FTC admitted that "[t]here is nothing out there for a company to look to." Trans. 9:13-18.

PUBLIC

The FTC admits that it has never promulgated data-security regulations, guidance, or standards under Section 5: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act...for financial institutions." Trans. 10:11-15.

When asked about other sources of data-security standards, FTC said: the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC also stated that "public statements made by the Commission" and so-called "educational materials" were standards. *Trans.* 9:23-25. And finally the FTC argued that "the IT industry...has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7.

In response to LabMD's written discovery requesting documents relating to the standards the FTC enforces regarding data-security, the FTC produced thousands of pages of consent decrees, reports, PowerPoint presentations, and articles from the FTC's website, including many in Spanish. Ltr. from L. VanDruff, dated Jan. 27, 2014, attached hereto as Exh. 6 (showing that the FTC produced thousands of documents responsive to Request 10, which requested documents pertaining to the standards the FTC enforces); Ltr. from L. VanDruff, dated Mar. 3, 2014, attached hereto as Exh. 7 (same); Example of Production, attached hereto as Exh. 8.

PUBLIC

At the hearing, the ALJ asked: "Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?" The FTC responded "No." Trans. 22:10-13.

The FTC also admits that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17.

STANDARD OF REVIEW

Commission Rule 3.24 provides that "[a]ny party ... may move ... for a summary decision in the party's favor upon all or any part of the issues being adjudicated." 16 C.F.R. § 3.24(a)(1). Rule 3.24 further provides that if the Commission determines that there is no genuine issue as to any material fact regarding liability or relief, it shall issue a final decision and order. 16 C.F.R. § 3.24(a)(2).

When a motion for summary decision is made and adequately supported, "a party opposing the motion may not rest upon the mere allegations or denials of his or her pleading; the response, by affidavits or as otherwise provided in this rule, must set forth specific facts showing that there is a genuine issue of material fact for trial." 16 C.F.R. §3.24(a)(3). Once the moving party has adequately supported its motion, the nonmoving party must "do more than simply show that there is some metaphysical doubt as to the material facts." *In re North Carolina State Board of Dental Examiners*, 151 F.T.C. 607, 611 (2011) (internal citations and quotation marks omitted). The non-moving party must instead establish "specific facts showing that there is a genuine issue for trial." *Id.* (internal citations and quotation marks omitted); *see also* 16 C.F.R. § 3.24(a)(3). And "[w]here the record taken as a whole could not lead a rational trier of fact to find for the nonmoving party, there is no 'genuine issue for trial.'" *North Carolina*, 151 F.T.C. at 611 (internal citations and quotation marks omitted).

PUBLIC

ARGUMENT

I. SECTION 5's UNFAIRNESS PROVISION DOES NOT AUTHORIZE FTC TO CREATE A COMMON LAW OF PHI DATA SECURITY.

LabMD believes that FTC lacks Section 5 "unfairness" authority to regulate data-security generally, and specifically for PHI. *See* Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD") (Nov. 12, 2013); Reply to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("Reply to MTD") (Dec. 2, 2013). For the reasons set forth therein, the Commission's MTD Order is wrongly decided and summary decision for LabMD should be granted.[3]

The PHI in LabMD's possession is information that patients voluntarily gave to their doctors, who in turn, voluntarily provided this information to LabMD. Even so, the Commission claims that Section 5's unfairness authority sanctions the use of legal process against LabMD "to protect consumers from unwanted privacy intrusions..." MTD Order at 1. This claim, however, conflicts with the United States government's long-standing assertion that consumers who voluntarily provide personal information to third parties lose their privacy rights because the information in question, once given, belongs to the receiver and not the consumer. *See, e.g.,*

[3] Worldwide Corporation, Order on Mot. to Dismiss No. 2:13-CV-01887-ES-JAD, Dkt. 181,(D. N.J., Apr. 7, 2014)("Wyndham Order on Mot. to Dismiss") is not a PHI case. But it too is wrongly decided. Using a tautology - FTC has sweeping authority because it has sweeping authority - the court dodged the hard legal question: Does FTC's roughly fifty consent orders and internet posts constitute adequate fair notice? The district court noted the "rapidly-evolving nature of data security" and quoted *General Electric v. Gilbert*, 429 U.S. 125 (1976) for the proposition that "the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance." Wyndham Order on Mot. to Dismiss at 24. However, the court omitted the very next sentence: "The weight of such a judgment in a particular case will depend upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control." *See Gilbert*, 429 U.S. at 142 (citation omitted).

The Wyndham court noted that Congress has prescribed a three-part standard for unfairness but fail utterly to assess whether FTC has thoroughly or rigorously applied that standard, or whether the approach it has taken is really an end run of Congressional efforts to prevent unelected bureaucrats from avoiding accountability and transparency. The idea that FTC has the unbounded power to create a law of data security, binding on all companies economy-wide using nothing more than ad hoc consent orders and unilateral internet posts and without any meaningful public scrutiny or input, cannot be seriously defended. But such was the court's ruling.

PUBLIC

Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint, *ACLU, et al., v. Clapper, et al.,* Case No. 13 Civ. 3994 (WHP), Dkt. No. 33 at 32-33 (Aug. 26, 2013)("Gov. Motion") citing *Smith v. Maryland,* 442 U.S. 735, 743-44 (1979)("a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); *United States v. Miller*, 425 U.S. 435, 440-41 (1976)(rejecting a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, inasmuch as the bank was a party to the transactions, the records belonged to the bank).[4] In other words, FTC has attacked LabMD for "misusing" its own property.

Through HIPAA, Congress created ***enforceable privacy rights*** in PHI and authorized HHS to promulgate binding regulations governing medical providers that handle it. But as FTC claims this case has nothing to do with HIPAA, MTD Order at 12 ("To be sure, the Commission cannot enforce HIPAA and does not seek to do so"), it therefore runs into a thick wall of federal arguments that conflict with FTC's foundational premise: that consumers who voluntarily give PHI to medical providers have some protectable privacy or other interest in that information beyond that which Congress authorized HHS to carve out under HIPAA. Consequently, without proof of deception, the FTC's section 5 authority does not extend to the regulating PHI. *New Hampshire v. Maine,* 542 U.S. 742, 749-50 (2001).

---

[4]The government argued:

> In *Smith v. Maryland*....the Court reasoned, even if a subscriber harbored a subjective expectation that the phone numbers he dialed would remain private, such an expectation of privacy would not be reasonable, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

Gov. Motion at 33 (citations omitted). Thus, "Courts have followed Smith to find no reasonable expectation of privacy in email "to/from" and Internet protocol ("IP") addressing information, in text message addressing information, and in subscriber information, such as subscribers' names, addresses, birthdates, and passwords, communicated to system operations and Internet service providers." *Id.* (citations omitted).

PUBLIC

II. THE FTC HAS FAILED THE FAIR NOTICE TEST AND VIOLATED DUE PROCESS.

The FTC may have broad power under Section 5, but even the broadest of bureaucratic powers have constitutional limits. Due process prohibits the FTC from using legal process against LabMD without first providing fair notice, a doctrine that is "[a] fundamental principle in our legal system [requiring] that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). If a person acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects the entity to conform, the agency has not provided fair notice. *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995). Administrative law has thoroughly incorporated this constitutional fair notice requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *See Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007)("Even if the Secretary's interpretation was reasonable, announcing it for the first time in the context adjudication deprives Petitioners of fair notice); *Satellite Broadcasting Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)(traditional concepts of due process incorporated into administrative law preclude agencies from penalizing private parties for violating rules without first providing adequate notice of their substance).

FTC has taken a variety of inconsistent positions on the matter of fair notice, ranging from "it is not obligated to provide adequate notice" to "Section 5(n) provides adequate notice." As discussed below, each of these varying positions contradicts black letter law. Here, FTC seeks to impose PHI data-security standards that conflict with HIPAA. It thereby violates LabMD's due process rights as no such separate and additional PHI data-security standards were known to exist by LabMD or any other Covered Entity.

PUBLIC

Because the FTC has failed to provide constitutionally adequate notice to LabMD of the PHI standards it seeks to enforce, LabMD's motion for summary decision should be granted.

A. FTC Failed To Provide Constitutionally Adequate Notice Of the Data Security Standards it Currently Seeks to Impose on Entities that Possess PHI

This case is an instance in which the FTC claims the power to create its own "common law" PHI data-security requirements which are more stringent and inconsistent with those created by HHS.

For example, in *In the Matter of Rite Aid Corporation,* the FTC began its investigation following news reports about Rite Aid pharmacies using open dumpsters to discard trash containing consumers' personal information such as pharmacy labels and job applications. At the same time, HHS began investigating the pharmacies' handling of PHI. *See* FTC Dkt. C-4358, http://www.ftc.gov/news-events/press-releases/2010/07/rite-aid-settles-ftc-charges-it-failed-protect-medical-and. Eventually, FTC alleged that Rite Aid failed to protect "sensitive financial and medical information" while HHS alleged that it failed to protect PHI. *Id.* Rite Aid settled with both FTC and HHS. *Id.* FTC required Rite Aid to protect personal information while HHS's settlement required Rite Aid to protect PHI. *Id; see also In the Matter of CVS Caremark, FTC* Dkt. C-4259, http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial (involving PII and PHI data-security, where FTC used its Section 5 authority for PII and HHS used its HIPAA authority for PHI).

The FTC has taken the position that the *Rite Aid* and *CVS* cases are part of the developing common law which establishes it as having concurrent jurisdiction to enforce HIPAA. However, it is clear that those two cases involve entities that do not deal exclusively with PHI. Taken together, FTC's "common law" and the Commission's ruling in its MTD Order demonstrate that HHS has always been responsible for PHI data-security standards and that HIPAA, not Section

PUBLIC

5's general unfairness provision, controls in this case. It is perhaps arguable through the its involvement in the *Rite Aid* and *CVS* cases, that the FTC has demonstrated that it has complementary jurisdiction to enforce PHI data-security using HIPAA standards, however the FTC has denied having such authority. Thus, there can be no dispute that the FTC's claim in this case that Section 5 authorizes it to over-regulate HIPAA and create a new law "common law" of PHI data-security is newly baked. Companies like LabMD that maintain only PHI could not have known that the FTC had decided HIPAA compliance was not enough. Simply, the FTC's prior involvement in cases such as *Rite Aid* and *CVS*, combined with its three-year investigation and creation of ex post facto "springing standards" that, by happenstance, LabMD failed to meet, is insufficient to meet LabMD's constitutional due process right to fair notice..

Instead of enforcing HIPAA standards, which provide fair notice and have been properly promulgated through notice and comment rulemaking, the FTC has now decided to hold companies like LabMD to never-before-seen and ever-changing standards that it concocts after the alleged offense has occurred. Even the FTC admits that by using its Section 5 "unfairness" authority in this manner, it is seeking to enforce standards *ex post facto*. Ohlhausen Statement at 11-13, attached as Exh. 9.

Here, FTC is seeking to enforce standards that its expert, Professor Raquel Hill, devised after reviewing three years worth of material the FTC collected during its investigation of LabMD along with testimony and materials collected during discovery. *See* Complaint Counsel's Expert Report of Professor Raquel Hill, generally, attached hereto as Exh. 5. FTC's determination to fabricate its own standards may explain why it has taken varying and inconsistent positions throughout this case.

PUBLIC

1. The FTC is obligated to provide adequate notice of the standards it seeks to enforce.

Despite the fair notice doctrine's robust application in a variety of administrative actions, *see e.g. Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007)("Even if the Secretary's interpretation was reasonable, announcing it for the first time in the context adjudication deprives Petitioners of fair notice), the FTC has taken the position that it is not obligated to provide any fair notice at all because agencies have broad discretion to "address an issue by rulemaking or adjudication." MTD Opp'n at 15. This position was recently highlighted in the deposition of the Bureau of Consumer Protection's Rule 3.33 witness, Daniel Kaufman. Here, Respondent's counsel asked Mr. Kaufman a series of questions related to published standards that the Bureau sought to enforce against LabMD; however, Complaint Counsel instructed the witness not to respond to any of these questions. Deposition of Daniel Kaufman, Apr. 14, 2014 at 115-139, attached hereto as Exh. 10.

For example Respondent's Counsel asked Mr. Kaufman, "Based on the allegations in paragraph 10(a), my question is has the Bureau or the FTC published, and by published I mean made available to the public, the standard that it requires for a comprehensive information security program for companies like LabMD to have in place?" Complaint Counsel objected to the question stating, "I object to the question because it exceeds the bounds of the Court's March 10th, 2014 protective order, and I am instructing Mr. Kaufman to not answer the question. . ." Deposition of Daniel Kaufman, Apr. 14, 2014 at 119, attached hereto as Exh. 10.

Complaint Counsel has taken the position that it is not required to inform LabMD of the data security standards applicable to this case despite the ALJ's March 10, 2014, Order. ("Complaint Counsel has not demonstrated that Topic 2 is entirely outside the scope of

PUBLIC

discovery, so as to bar any and all deposition testimony within its scope, and Respondent has articulated a valid line of inquiry.")

Alternatively, the FTC has argued that it is not obligated to provide fair notice because it is not seeking "criminal punishment or civil penalties for past conduct." MTD Order at 16. To the contrary, it is well settled that administrative agencies must provide fair notice not only when they pursue criminal or civil penalties, but also in cases in which they seek other kinds of burdensome relief. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1354-55 (D.C. Cir. 1998) (holding that fair notice is required when the government seeks a product recall); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002)(forfeiture); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000) (license revocation). If the FTC is successful on the merits of its case, then LabMD will be subject to an array of burdensome financial requirements. The FTC typically reserves the right to order or seek additional relief as it sees fit, including, but not limited to permanent injunctive relief, restitution, disgorgement, rescission or reformation of contracts, payment of monetary damages, and (likely) decades of intrusive and costly external monitoring. These are "'sufficiently grave sanction[s]' such that the duty to provide notice is triggered." Chrysler, 158 F.3d at 1355.

2. *Section 5(n) does not constitute fair notice of the standards the FTC seeks to enforce against LabMD.*

FTC has argued that the plain text of Section 5(n) somehow adequately provides "a person of ordinary intelligence fair notice of what is prohibited." MTD Order at 17-18. Section 5(n) provides:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

PUBLIC

However, this section does no more than announce in general terms what types of consumer injuries fall within the FTC's jurisdiction. *See* 15 U.S.C. § 45(n). It does not provide any guidance whatsoever about the nature or kinds of data-security standards, methodologies, procedures, or processes a company must adopt in order to be compliant, nor does it provide even general guidance about how it measures the performance of a company's data security practices. FTC thus stretches its own credibility by arguing that the text of Section 5(n) itself somehow "provide[s] greater certainty for businesses." MTD Order at 5. Surely if the FTC believed this to be true, Professor Hill's expert analysis on whether LabMD provided "reasonable and appropriate security for Personal Information within its computer network" would have mentioned and analyzed Section 5(n). However, this opinion is devoid of any mention of Section 5(n). Complaint Counsel's Expert Report of Professor Raquel Hill, attached hereto as Exh. 5.

3. Consent Decrees, Negotiations, Public Statements made by the Commission, Reports, PowerPoint Presentations, and Articles on the FTC's website do not constitute fair notice of the standards the FTC seeks to enforce.

In LabMD's written discovery to the FTC, it requested the following documents:

> 8. All documents sufficient to show what data-security standards are currently used by the FTC to enforce the law under Section 5 of the Federal Trade Commission Act.
>
> 9. All documents sufficient to show what changes occurred in the data-security standards used by the FTC to enforce the law under Section 5 of the Federal Trade Commission Act from 2005 to present and the dates on which these standards changed.
>
> 10. All documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act form 2005 to present.

PUBLIC

See FTC's Discovery Responses, attached in relevant part hereto as Exh. 11. In response to these discovery requests, Complaint Counsel produced thousands of pages of documents which included consent decrees, industry guidance, PowerPoint presentations, and articles on the FTC's website. *Id.*; *see also*, Ltr. from L. VanDruff, dated Jan. 27, 2014, attached hereto as Exh. 6; Ltr. from L. VanDruff, dated Mar. 3, 2014, attached hereto as Exh. 7. To the extent that Complaint Counsel wishes to assert that these materials provide adequate notice, it is incorrect.

First, the Commission cannot claim that a diffuse collection of Commission consent orders establish generally-applicable data-security standards or put the public on notice thereof. FTC cannot regulate by consent orders. *See Gen. Elec. Co. v. EPA*, 290 F.3d 377, 382-83 (D.C. Cir. 2002)(holding that agency guidance document that imposes binding duties and obligations violates the APA). Consent orders "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement." *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). Moreover, consent orders do not bind the Commission or restrict its discretion in future actions and statements that do not constrain governmental authority do not provide the fair notice that due process requires. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999). Indeed, in Section 5 itself Congress *specifically barred* the Commission from binding third parties by consent order: the Commission is statutorily prohibited from enforcing a "consent order" against anyone that is not a party to it. 15 U.S.C. § 45(m)(2); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir. 2007)("Indeed, the FTC Act...with regard to consent orders...specifically provides that the Commission cannot enforce them against non-parties.").

Moreover, general statements of policy, such as industry guidance, power point presentations, and articles on the FTC's website, are prospective and do not create obligations

PUBLIC

enforceable against third parties like LabMD. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a...policy statement announces the agency's tentative intentions for the future"); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006)(in holding agency manuals to be nonbinding, the court said that "it is particularly noteworthy that NPS did not issue its management policies through notice and comment rulemaking under 5 U.S.C. § 553" because failure to do so is evidence that the material in question was not supposed to be a rule binding regulated companies' conduct).

Tellingly, the FTC's expert, Professor Raquel Hill, who opined on "reasonable and appropriate security for Personal Information within its computer network" never consulted any of the materials that FTC purports it is "using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act." Complaint Counsel's Expert Report of Professor Raquel Hill at Appendix B, attached hereto as Exh. 5. Rather Ms. Hill's report consists of entirely new and never-disclosed metrics. *Id.*

III. If FTC May Over-Regulate HIPAA, It May Over-Regulate All Other Regulated Areas Affecting Consumers.

If FTC may lawfully over-regulate HHS, add to HIPAA and attack LabMD using its Section 5 unfairness authority, then, upon its determination that a given practice "is reasonably likely to cause harm to consumers," it may lawfully over-regulate drinking water governed by the Safe Drinking Water Act or food products subject to "standards of identity" established by the Food and Drug Administration such as Swiss cheese or spring water. It may over-regulate hazardous waste management practices subject to the Resource Conservation and Recovery Act and long-standing Environmental Protection Agency regulations. And, it may over-regulate in the fields of employment law or nuclear energy or any other myriad of regulated areas which

PUBLIC

naturally could harm consumers. Clearly then, there is no end to FTC's power and Section 5, most recently amended by Congress in 1994 to limit the Commission's power, is instead a gateway to total regulatory authority. Congress never intended FTC to have such sweeping and over-riding authority to intervene and superimpose new and additional requirements on entities, especially when properly promulgated regulations already exist and adequate notice has not been provided.

IV. Even If FTC Provided LabMD Fair Notice, HIPAA Controls.

In *Credit Suisse Securities (USA) LLC v. Billings*, 551 U.S. 265 (2007), the United States Supreme Court set forth the factors to consider to determine when a specific regulatory regime displaces, or implicitly precludes enforcement under, a more general and earlier enacted regulatory scheme. The Court held that the securities laws were "clearly incompatible" with the antitrust laws and therefore, held that the antitrust claims were precluded by the securities law regulatory regime. While *Credit Suisse* specifically addressed the interplay of securities regulation and antitrust law, the test and its underlying logic apply here.

The issue in *Credit Suisse* was whether a plaintiff could file antitrust claims against investment banks that had formed syndicates and engaged in other practices to form markets for initial public offerings that were actively regulated under the securities laws. 551 U.S. at 269-70. The Supreme Court applied a four-factor test to determine whether such incompatibility existed:

> [I]n finding sufficient incompatibility to warrant an implication of preclusion, have treated the following factors as critical: (1) the existence of regulatory authority under the securities law to supervise the activities in question; (2) evidence that the responsible regulatory entities exercise that authority; and (3) a resulting risk that the securities and antitrust laws, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct . . .. We also note (4) in *Gordon* and *NASD* the possible conflict affected practices that lie squarely within an area of financial market activity that the securities law seeks to regulate.

PUBLIC

Credit Suisse, 551 U.S. at 275-76. These factors support a finding that HIPAA regulation of data security is incompatible with FTC over-regulation.

First, HIPAA directly applies and delegates rulemaking and standard setting authority to HHS. Indeed, HHS has adopted data privacy and data security rules, which it routinely enforces. *See, e.g.*, 42 U.S.C. §1320d(3)-(4) (defining terms); 45 C.F.R. § 160.103 (same); 42 U.S.C. § 1320d-2(d)(1) (establishing "Security standards for health information" and providing HHS with enforcement authority); 65 Fed. Reg. 82,462 (Dec. 28, 2000) (HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334 (Feb. 20, 2003) (HHS's HIPAA Security Rule); *see also* 78 Fed. Reg. 5,566 (Jan. 25, 2013) (HHS's HITECH Rule). These rules address the same activities that are the subject of this case.

Second, dual enforcement is resulting in (and will continue to result in) conflicting guidance and requirements. The best illustration of conflict is that LabMD's compliance with the HIPAA is not a defense to the newly created FTC regulations. Rather, FTC deems regulatory compliance to be irrelevant to, much less a defense against, Section 5 unfairness claims. *See, e.g.*, FTC's Mot. to Dismiss, *LabMD, Inc. v. Federal Trade Commission*, No. 1:14-CV-810-WSD, N.D. Georgia Dkt 18, at 27 (arguing that HHS's regulations implanting HIPAA serve to "establish a *minimum* level of security that covered entities must meet" (internal quotation omitted, emphasis in original)). This disdain creates inherent conflict and confusion among HIPAA Covered Entities

HHS's PHI data-security standards differ in material ways from the FTC's purported standards. FTC's "standards," at least as articulated by its expert, introduce additional security principles that are difficult to reconcile with Administrative, Technical and Physical main structure of the HIPAA security rule. For example, they are not scalable in accordance with the

PUBLIC

Security Rule,[5] and do not account, as required by HIPAA, for the needs and capabilities of small health care providers and rural health care providers.[6] The recommendation for file integrity monitoring requires expertise to implement and configure these solutions and can be even more resource intensive to understand, investigate and resolve alerts from the solution.

Other FTC "standards" that are more prescriptive than HIPAA or inconsistent with HHS guidance, include encryption at rest (an addressable requirement of 164.312(a)(1)), encryption in transit (an addressable requirement of 164.312(e)(1)), intrusion detection (not addressed specifically by the Security Rule), virus protection (an addressable requirement of 164.308(a)(5)(ii)(B)), firewalls (not addressed specifically by the Security Rule), penetration testing (not addressed by the Security Rule), and file integrity monitoring (not addressed specifically by the Security Rule). The electronic health record certification requirements published for HHS for Meaningful Stage 2 in 2012 do not even require this level of encryption for all PHI stored by the system. In addition, tools such as intrusion detection and file integrity monitoring systems require experienced and committed technical resources to configure and manage.

FTC's "standards" presume a level of technical knowledge generally not available to small health care providers and conflict with HHS guidance. For example, FTC's expert almost exclusively focuses on technologies or technical processes for the risk assessment process (i.e., antivirus applications, firewalls, various types of vulnerability scans, intrusion detection systems, penetration tests, file integrity monitoring, and other measures). This is inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process.

---

[5] 68 Fed. Reg. 8,334, 8,335 (Feb. 20, 2003). In the preamble to the HIPAA Security Rule, HHS emphasizes that the Rule must be "scalable, so that it can be effectively implemented by covered entities of all types and sizes," and notes further that "[s]ince no comprehensive, scalable, and technology-neutral set of standards currently exists, we proposed to designate a new standard, which would define the security requirements to be fulfilled." *Id.* at 8,341.

[6] 42 U.S.C. § 1320d–2(d)(1)(A)(v).

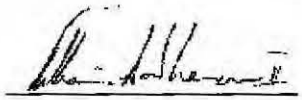
PUBLIC

If health care providers are going to be held to a compliance standard that is simply an expert's opinion of best practices in information security at any point in time, when that expert standard exceeds the compliance standard developed by notice and comment rulemaking under HIPAA, then the standard developed under HIPAA is made effectively meaningless, null and void. *See also* Declaration of Cliff Baker, *LabMD, Inc. v. Federal Trade Commission*, No. 1:14-CV-810-WSD, N.D. Georgia Dkt. No. 17-6, attached hereto as Exh. 12.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion for Summary Decision and ORDER that the Complaint be dismissed with prejudice.

Respectfully submitted,



Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20006
Telephone: 202.372.9120
Fax: 202.372.9141

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: April 21, 2014

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	

[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S MOTION FOR SUMMARY DECISION

This matter came before the Commission on April 21, 2014, upon a Motion for Summary Decisions ("Motion") filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rules 3.22 and 3.24, 16 C.F.R. §§ 3.22 and 3.24, for an Order granting summary decision in favor of LabMD on all counts set forth in the Federal Trade Commission's ("FTC") administrative Complaint against LabMD, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (Aug. 28, 2013). Having considered LabMD's Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that LabMD's Motion is GRANTED.

ORDERED:

Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Joshua D. Wright
Commissioners

Date:

CERTIFICATE OF SERVICE

I hereby certify that on April 21, 2014, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-113
Washington, DC 20580

I certify that I caused to be hand-delivered twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

I also certify that I delivered via electronic mail and caused to be hand-delivered a copy of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

Dated: April 21, 2014

By: /s/ Michael D. Pepson
Michael D. Pepson

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: April 21, 2014 By:/s/William A. Sherman, II

2962021v2

EXHIBIT 1

In the Matter of:

LabMD, Inc.

November 21, 2013
Robert J. Boback

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

Q. When did Tiversa download CX 10?

A. I believe it was in February of 2008.

Q. Has CX 10 changed in any way since Tiversa downloaded it?

A. No.

A.

EXHIBIT 2

Forthcoming in *Financial Cryptography and Data Security*, February 22-25, 2009.

Data Hemorrhages in the Health-Care Sector[1]

M. Eric Johnson

Center for Digital Strategies
Tuck School of Business
Dartmouth College, Hanover NH 03755
{M.Eric.Johnson}@dartmouth.edu

Abstract. Confidential data hemorrhaging from health-care providers pose financial risks to firms and medical risks to patients. We examine the consequences of data hemorrhages including privacy violations, medical fraud, financial identity theft, and medical identity theft. We also examine the types and sources of data hemorrhages, focusing on inadvertent disclosures. Through an analysis of leaked files, we examine data hemorrhages stemming from inadvertent disclosures on Internet-based file sharing networks. We characterize the security risk for a group of health-care organizations using a direct analysis of leaked files. These files contained highly sensitive medical and personal information that could be maliciously exploited by criminals seeking to commit medical and financial identity theft. We also present evidence of the threat by examining user-issued searches. Our analysis demonstrates both the substantial threat and vulnerability for the health-care sector and the unique complexity exhibited by the US health-care system.

Keywords: Health-care information, identity theft, data leaks, security.

1 Introduction

Data breaches and inadvertent disclosures of customer information have plagued sectors from banking to retail. In many of these cases, lost customer information translates directly into financial losses through fraud and identity theft. The health-care sector also suffers such data hemorrhages, with multiple consequences. In some cases, the losses have translated to privacy violations and embarrassment. In other cases, criminals exploit the information to commit fraud or medical identity theft.

[1] Experiments described in this paper were conducted in collaboration with Tiversa who has developed a patent-pending technology that, in real-time, monitors global P2P file sharing networks. The author gratefully acknowledges the assistance of Nicholas Willey. This research was partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

EXHIBIT 3

In the Matter of:

LabMD, Inc.

December 17, 2013
Detective Karina Jestes

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

25

1

12

29

1 the document that's been produced as CX0085.
2 A Okay.
3 **Q Are the documents that appear at CX0085 a true**
4 **and accurate copy of the materials that you seized at**
5 **[redacted] that referenced LabMD?**
6 A Yes.
7 **Q Are these the documents -- excuse me.**
8 **Are the documents that appear at CX0085 a true**
9 **and accurate copy of the materials that you provided to**
10 **FTC staff?**
11 A Yes.
12 **Q Did you book CX0085 into evidence?**
13 A Yes.
14 **Q Explain the process by which information**
15 **collected during an investigation is booked into evidence.**
16 A When an officer retrieves the evidence from a
17 scene, basically, it's maintained under their control
18 until it is then transported to the evidence section where
19 it's inputted into a computer and then put into a locked
20 container for the evidence technicians to then find a
21 permanent place for.
22 **Q That process occurred with respect to the**
23 **document that appears at CX0085; is that correct?**
24 A Yes.
25 **Q Is booking into evidence information that an**

30

1 **officer collects, during a criminal investigation, done in**
2 **the ordinary course of the Sacramento Police Department's**
3 **activities?**
4 A Yes.
5 **Q I'm handing you a document that has been marked**
6 **as CX0087.**
7 **(Exhibit CX0087 was marked for**
8 **identification.)**
9 BY MS. VANDRUFF:
10 **Q I'm going to ask you to please take a moment to**
11 **review that.**
12 A Okay.
13 **Q What is CX0087?**
14 A "Day Sheet Transaction Detail" from LabMD, and
15 it's marked that it's a copy, and then there's a number at
16 the top that's the evidence control number for this
17 document.
18 **Q What is an evidence control number?**
19 A When items of evidence are booked from the scene
20 of the crime, they're each given a unique number; so this
21 number is -- well, "755867" would be the kind of group
22 number that items of evidence can be logged in under, and
23 then each item is given a specific number; so this one is
24 "6."
25 **Q Can you tell whether CX0087 was booked into**

31

1 **evidence?**
2 **Let me ask the question differently,**
3 **Detective Jestes.**
4 **Does the presence of the control number,**
5 **755867-6, tell you whether or not the document that has**
6 **been marked as CX0087 was booked into evidence?**
7 A Yes, it was.
8 **Q Is the document that appears at CX0087 a true and**
9 **accurate copy of the booked evidence, 755867, Item 6?**
10 A Yes.
11 **Q Did you book CX0087 in your ordinary course of**
12 **your duties as a detective at the**
13 **Sacramento Police Department?**
14 A Yes.
15 **Q I'm handing you a document that has been marked**
16 **as CX0088.**
17 **(Exhibit CX0088 was marked for**
18 **identification.)**
19 BY MS. VANDRUFF:
20 **Q I'm going to ask you to take a moment, please,**
21 **and review the document.**
22 A Okay.
23 **Q What is CX0088?**
24 A It's Item of Evidence No. 55867-7.
25 **Q Was CX0088 booked into evidence?**

32

1 A Yes.
2 **Q Did you book CX0088 in the ordinary course of**
3 **your duties as a detective of the**
4 **Sacramento Police Department?**
5 A Yes.
6 **Q With respect to CX0088, is CX0088 a true and**
7 **accurate copy of what you booked into evidence as**
8 **755867, Item 7?**
9 A Yes.
10 **Q I'm handing you a document that has been marked**
11 **as CX0086.**
12 **(Exhibit CX0086 was marked for**
13 **identification.)**
14 BY MS. VANDRUFF:
15 **Q I'm going to ask you to please take a moment and**
16 **review the document.**
17 A Okay.
18 **Q What is CX0086?**
19 A A declaration of custodian of records.
[redacted]

33

1 **Q Does CX0086 relate to**
2 **Booked Evidence Case No. 755867?**
3 A Yes.
4 **Q Does CX0086 relate specifically to the documents**
5 **that we have just discussed that appear at CX0087 and**
6 **0088?**
7 A Yes.
8 MS. HARRIS: Pardon me.
9 I'm going to interpose an objection that this
10 witness is not the proper witness to lay a foundation for
11 the records that we've just discussed. [redacted] is
12 the proper person to lay the evidentiary foundation.
13 BY MS. VANDRUFF:
14 **Q Let's return to CX0087.**
15 **What information is contained in CX0087?**
16 A The top of the sheet says
17 "Day Sheet Transaction Detail LabMD, Inc.," and then there
18 is what appears to me to be names of possibly clients with
19 social security numbers and then a billing number, a date,
20 and then there's an amount -- a monetary amount.
21 **Q Based on your training and experience, where are**
22 **the social security numbers that appear on CX0087?**
23 A To the left of the name.
24 **Q Why do you conclude that those are social**
25 **security numbers?**

34

1 A Because there's three numbers, a dash, two
2 numbers, a dash, and then four numbers, which in my
3 training and experience is a social security number.
4 **Q Why did you book CX0087 into evidence?**
5 A Because I felt that there was evidence of
6 identity theft.
7 **Q Based on your training and experience, what led**
8 **you to that conclusion?**
9 A Part of identity theft is having the personal
10 identifying information of another, and none of these
11 people listed here or their social security numbers were
12 supposed to be in that house. These documents are other
13 people's identifying information. Ms. [redacted] and
14 Mr. [redacted] should not have had possession of this.
15 **Q Did the presence of other documents that related**
16 **to individuals who were neither Mr. [redacted] nor**
17 **Ms. [redacted] affect your opinion about the significance**
18 **of the document that appears at CX0087?**
19 A Sorry. Could you repeat that one?
20 MS. VANDRUFF: I'm going to ask the reporter to
21 repeat that for me.
22 (Record read.)
23 THE WITNESS: Yes.
24 BY MS. VANDRUFF:
25 **Q In what way?**

35

1 A The other items that were found in this home such
2 as checks and utilities with other people's information on
3 them was also evidence of identity theft; so I believed
4 that this information as well could have been used for
5 financial gain or some kind of narcotics gain by these
6 people by having other people's social security numbers
7 and names in their possession.
8 **Q Okay. I'd ask you to return your attention**
9 **please to the document that appears at CX0088.**
10 **What information is contained in CX0088?**
11 A These are copies of checks written to LabMD and
12 signed by the person whose name is on the check.
13 **Q What types of personal information are included**
14 **in the checks that appear in CX0088?**
15 A Names, addresses, phone numbers, account numbers,
16 and signatures.
17 **Q In addition to the information that you've just**
18 **described, there are handwritten notations on some of the**
19 **pages -- for example, pages 4, 7, and 9.**
20 **What is the significance of the notations that**
21 **appear on pages 4, 7, and 9 of CX0088?**
22 MS. HARRIS: Objection to the extent it calls for
23 speculation.
24 THE WITNESS: It looks like there are social
25 security numbers written on those checks.

36

1 BY MS. VANDRUFF:
2 **Q What is the basis of that conclusion?**
3 A Again, the way the number is written. There's
4 three digits, a dash, two digits, a dash, and then four
5 digits.
6 **Q In your training and experience, what's the**
7 **significance of that sequence of numbers?**
8 A It would be a social security number.
9 **Q There are notations that appear on other pages --**
10 **for example, page 1, 5, and 8.**
11 **What is the significance, if you know, of those**
12 **notations?**
13 MS. HARRIS: Objection. Calls for speculation.
14 THE WITNESS: Some of them look like monetary
15 amounts, and then it looks like there's a phone number
16 written on one, and I don't know -- I'd have to do more
17 comparing of another documents to see if they correlated.
18 BY MS. VANDRUFF:
19 **Q Why did you book CX0088 into evidence?**
20 A These checks didn't have any connection to the
21 house we were at or the people who were residing there at
22 the time, and they should not have had in their possession
23 account numbers and other personal identifying information
24 from other people.
25 **Q So given that this -- that the document that**

53

[redacted]

24

[redacted]

[redacted]

56

1 MS. VANDRUFF: Objection to form.
2 THE WITNESS: Correct.
3 BY MS. HARRIS:
4 **Q With respect to what has been marked by complaint**
5 **counsel as CX0088 this morning, did you attempt to contact**
6 **any of the people listed on these checks?**
7 A From what I remember of my investigation, I
8 looked and saw that none of them had a Sacramento
9 connection based on their information on the checks, and I
10 may have done a simple Google-type search to see if they
11 had a connection, but since it's not documented in my
12 report, there was no connection to these people to the
13 Sacramento Police Department.
14 **Q Do you have any evidence that any of the people**
15 **in CX0088 have been the victim of identity theft?**
16 A I do not have that information.
17 **Q So the LabMD documents which, again, have been**
18 **identified as CX0088 and CX0087 --**
19 MS. VANDRUFF: Counsel, I'm sorry to interrupt.
20 We've also marked as CX0085 the materials that
21 Detective Jestes provided initially to FTC staff. Just so
22 the record is clear, there are three separate exhibits
23 that relate to LabMD.
24 Excuse my interruption.
25

EXHIBIT 4

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S AMENDED RESPONSE TO LABMD, INC.'S FIRST SET OF REQUESTS FOR ADMISSION (NUMBERS 1-20)

Pursuant to Sections 3.31 and 3.32 of the Federal Trade Commission's Rules of Practice for Adjudicative Proceedings ("Rules of Practice"), Complaint Counsel hereby amends its responses to Respondent LabMD, Inc.'s First Set of Requests for Admission ("Respondent's Requests").

Complaint Counsel has not completed its discovery or its preparation for trial. Complaint Counsel's answers to Respondent's Requests are given without prejudice to Complaint Counsel's right to produce information relating to any subsequently discovered facts. Complaint Counsel reserves the right to assert additional objections to Respondent's Requests, and to amend or supplement these objections and responses as necessary after the close of discovery.

General Objections

The following General Objections apply to each of Respondent's Requests and are hereby incorporated by reference into each response. The assertion of the same, similar, or additional objections or the provision of partial answers in response to an individual Request does not waive any of Complaint Counsel's General Objections as to the other Requests.

PUBLIC

Response to Request for Admission No. 5

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. *See* Order Denying Respondent LabMD's Motion to Dismiss at 14, *In the Matter of LabMD, Inc.*, Docket No. 9357 (Jan. 16, 2014) ("information security is an ongoing process of assessing risk and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve.") (citation omitted). Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "industry standards."

Complaint Counsel denies the Request to the extent that it suggests that Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), requires Complaint Counsel to allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use.

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel otherwise admits Request for Admission No. 5.

Request for Admission No. 6

Admit that the FTC has no evidence to dispute that LabMD has never been accused of violating either the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH) or any regulations implementing those statutes, including but not limited to as 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013) (HHS HITECH rule).

PUBLIC

Response to Request for Admission No. 6

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request to the extent it seeks information protected from disclosure by the common interest, deliberative process, law enforcement, and work product privileges. Complaint Counsel further objects to this Request to the extent it seeks information outside its possession, custody or control. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Request for Admission No. 7

Admit that the FTC has not accused LabMD of violating any rules or regulations not specifically referenced within the four corners of the FTC's Complaint.

Response to Request for Admission No. 7

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 7.

PUBLIC

Request for Admission No. 8

Admit that HIPAA, HITECH, and regulations implementing those statutes are not mentioned in the FTC's Complaint.

Response to Request for Admission No. 8

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding.

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 8.

Request for Admission No. 9

Admit that the information contained in the "Day Sheets" and "P2P insurance aging file" referred to in paragraphs 20 and 21 of the Complaint constitute Protected Health Information (PHI), as that term is used in HIPAA, HITECH, and regulations implementing those statutes.

Response to Request for Admission No. 9

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request to the extent it seeks a legal conclusion regarding the application of HIPAA, HITECH and the regulations implementing those statutes.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits that the information contained

EXHIBIT 5

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

In the Matter of	)	
	)	
LabMD, Inc.,	)	Docket No. 9357
a corporation,	)	
Respondent.	)	
	)	

EXPERT REPORT OF RAQUEL HILL, PH.D.

TABLE OF CONTENTS

I. Introduction 1

II. Summary of Experience and Qualifications 2

III. Overview of Network Security Principles 4

- A. Background: Computer Networks 4
- B. Defense in Depth 8
- C. Principles for Assessing and Securing a Network 11

IV. LabMD's Network During the Relevant Time Period 13

V. Scope of Opinions 16

VI. Materials Considered in Forming Opinions 17

VII. Summary of Opinions 18

VIII. Opinions 19

- A. Comprehensive Information Security Program – Complaint ¶ 10(a) 19
- B. Risk Assessment – Complaint ¶ 10(b) 24
- C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c) 30
- D. Information Security Training – Complaint ¶10(d) 34
- E. Use of Authentication Related Security Measures – Complaint ¶10(e) 36
- F. Maintenance and Updating of Operating Systems– Complaint ¶10(f) 38
- G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g) 41

IX. Conclusion 46

EXPERT REPORT OF RAQUEL HILL, PH.D.

I. Introduction

1. I am a tenured professor of Computer Science at Indiana University with over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems.

2. The FTC has engaged me to testify as an expert in this litigation. As explained in more detail in Section V, below, Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information[1] within its computer network.

3. This report states my opinions and provides the justifications for those opinions. It also includes the following information:

- A summary of my experience and qualifications;
- An overview of network security principles and a description of LabMD's network; and
- A description of the materials that I considered in forming my opinions and conclusions.

4. Based on my review of the materials described in Section VI, below, and my experience described in Section II, below, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures. This conclusion covers the time period from January 2005 through July 2010

---

[1] For purposes of this report, Personal Information means individually identifiable information from or about an natural person including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number. See Complaint Counsel's February 19, 2014 Requests for Admission to LabMD, p. 2.

(Relevant Time Period); as I explain in Paragraph 48, below, from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period. In section VIII, below, I present my specific opinions that support this conclusion.

II. Summary of Experience and Qualifications

5. I have over 25 years of combined academic, research, and industrial experience in computing. I received my B.S. degree with Honors in Computer Science from the Georgia Institute of Technology. As an undergraduate, I worked as a Cooperative Education student with IBM and received my Cooperative Education Certificate for working a minimum of six academic quarters with IBM as an undergraduate. This cooperative education experience allowed me to apply the theories that I was learning in the classroom, but also enabled me to help fund my degree.

6. I also received my M.S. degree in Computer Science from Georgia Tech. As an M.S. student, I worked for several companies, including: Cray Research, Hayes Microsystems, and Nortel Networks. My M.S. degree was funded by Cray Research via an academic scholarship.

7. After completing my M.S. degree, I worked for three years with Nortel Networks, where I designed and implemented network protocols that enabled telephone switches to communicate with remote devices. These protocols sustained communications even when a communications channel failed.

8. In 1996, I left Nortel Networks to pursue a Ph.D. in Computer Science at Harvard University. At Harvard, I designed and implemented a quality of service protocol that enabled routers in the network to reserve bandwidth for audio and video applications using a light-weight signaling protocol. As a part of this work, I evaluated the protocol to determine the threats and

vulnerabilities and designed mechanisms to secure the reservation process. I received my Ph.D. in October 2002, and began working as a lecturer within the School of Electrical Engineering at the Georgia Institute of Technology, where I taught a course in Digital Circuits. After working at Georgia Tech for 9 months, I accepted a position as a Post-Doctoral Research Associate with a joint appointment in the Computer Science Department and the National Center for Super Computer Application (NCSA) at the University of Illinois, Urbana-Champaign. As a Post-Doc, I designed and implemented mechanisms to secure environments where mobile devices and sensors are an integral part of the computing space. These spaces are often referred to as pervasive or ubiquitous computing environments. One of the major challenges to securing such environments is to apply uniform security policies across devices that have varying computational, space, and battery limitations.

9. After completing a two-year assignment at the University of Illinois, I joined Indiana University as an Assistant Professor of Computer Science in 2005. I was promoted to Associate Professor with tenure in 2012. Over the years, I have designed and taught classes in information and systems security including: Analytical Foundations of Security, Trusted Computing, Computer Networks, and Data Protection. My research areas span the areas of system security and data privacy. I have published articles on various topics, including: quality of service in networking, security for pervasive computing environments, encryption-based access control, reputation systems, trusted computing, smartphone security, and privacy in research datasets. I have published over 25 peer-reviewed articles and abstracts and given 25 invited technical talks and panels.

10. I am currently on sabbatical at Harvard University, where I am a Visiting Scholar within the Center for Research on Computation and Society at the School of Engineering and Applied Sciences. I am continuing my data protection research with a specific focus on medical data.

11. A more extensive summary of my professional accomplishments and a list of all publications that I have authored within the last 10 years can be found in my *curriculum vitae*, a copy of which is attached to this report as Appendix A. I have not testified as an expert at trial or at deposition within the last four years.

12. I am being compensated at a rate of $150 per hour for my work in connection with this litigation.

III. Overview of Network Security Principles

A. Background: Computer Networks

13. In this section, I describe very basic network functionality at a high level to support my opinions. A network is a collection of workstations, laptop computers, servers, and other devices (computers) that are connected via some communications channel that is either wired or wireless. In commercial settings, data is usually passed between computers within a network via a switch or a router. A switch and router can be combined into one device.

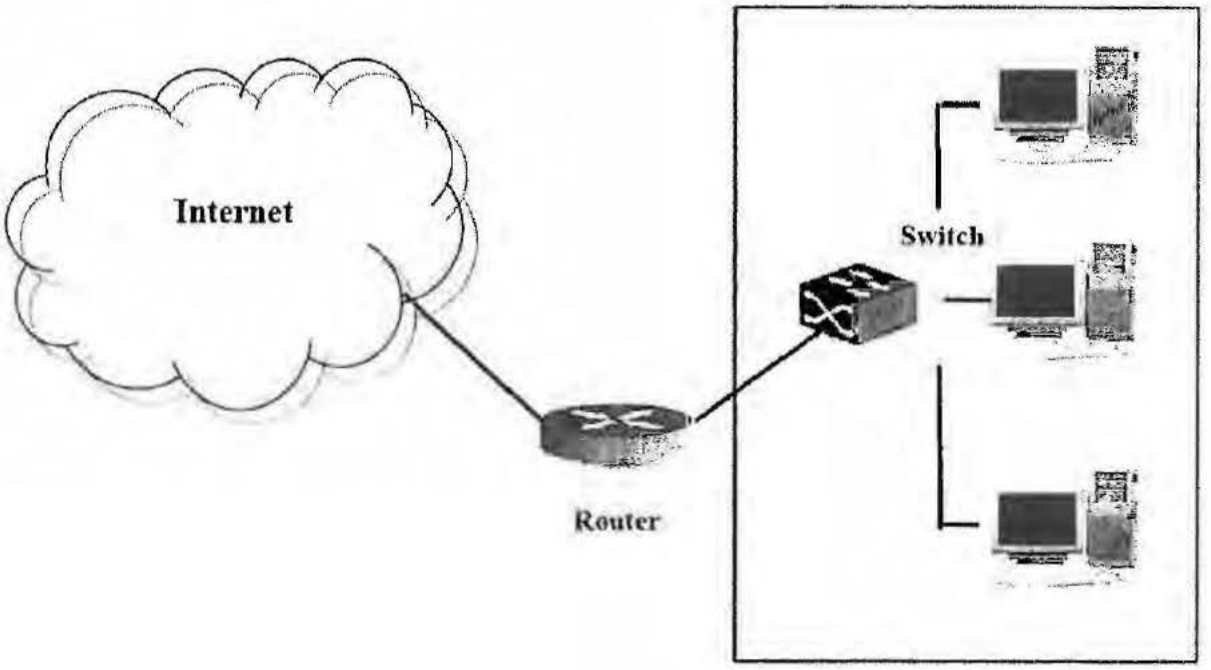
14. Computers use network interface cards (NIC) to connect to a network, and each NIC has a unique media access control (MAC) address. Each computer within a network is therefore uniquely identified by the MAC address of the computer's NIC. A computer's MAC address is not known outside of a computer's local area network (LAN).

15. A switch is a device that inspects incoming data to determine the destination MAC address and forwards the data to the computer with the specified MAC address.

16. A router is a device that connects networks. These networks may be of different types: wired vs. wireless, Ethernet vs. optical, etc. Routers forward data (in small units called packets) across the Internet using the Internet Protocol (IP) address of the destination computer. In doing so, the Domain Name System (DNS) is used to map a computer's hostname or a URL to an IP address. A computer's IP address is used by routers to forward data across the Internet to the specified destination network. Once the data reaches the destination network, the local switch uses the Address Resolution Protocol (ARP) to determine the MAC address of the computer that has the specified IP address. The switch passes the data to the destination computer.

17. **Figure 1** illustrates how a LAN may connect to the Internet. In the figure a switch connects the computers on the LAN and a router connects the LAN to the Internet. As noted in Paragraph 13, above, the function of the switch and the router can be combined into one device.

Figure 1: Connecting to the Internet



i. Network Addresses and Ports

18. In Paragraphs 13-16, I identified three types of addresses: Hostnames/URLs, IP addresses, and MAC addresses. DNS maps a hostname to an IP address, and ARP maps an IP address to a MAC address. The hostname and IP and MAC addresses are all needed to forward data to a specific computer. Once the data arrives at that computer, it must be sent to the application that is awaiting the information. The application is the ultimate recipient of any data that is sent to a computer on a network.

19. Applications are identified by numbers called ports. When data arrives at the destination, the receiving computer extracts the port number from the data and sends the data to the application that corresponds to that port number. Applications and their corresponding port numbers are the doors to computers and the networks to which the computers are connected. An application that contains a security vulnerability may allow an external entity to gain access to the LAN and any resources that are connected to the LAN. For this reason, it is important to ensure that all computers have been updated with all of the latest security patches for applications and related software

20. There are $2^{16} = 65{,}536$ possible ports on any computer. An open port is an open door to the computer, even when there is no application attached to the port. Therefore, it is important to close all unused ports on all computers. For example, when web access is not approved or authorized, ports 80 and 443 (which are typically used for web access) should be closed to prevent access to the computer through those ports.

ii. Firewalls and Intrusion Detection Systems

21. Firewalls are barrier mechanisms that are used to protect networks and individual computers. A firewall can be either a hardware device or a piece of software. It can be placed at a network gateway, or installed on a router or individual computer.

22. Firewalls can be configured to close all unused ports. When a port is closed, any data that arrives at the network or computer for that port will be discarded. Firewalls can also be configured to prevent and/or limit incoming connection requests. An incoming connection request is a request that originates from outside of the network but seeks to establish communication with a computer that is within the network. Only computers that are running authorized server applications should receive connection requests. A firewall, for example, could be configured to prevent all incoming connection requests for computers that are not running an authorized server application.

23. An intrusion detection system (IDS) is a device, typically another computer, that is placed inside a protected network to monitor activity in order to identify suspicious events. It can be either host-based or network-based. A host-based IDS runs on a single computer to protect that one host, while a network-based IDS is a stand-alone device that is attached to the network to monitor traffic throughout the network. An IDS acts as a sensor, like a smoke detector, that raises an alarm if specific things occur. It may perform a variety of functions including: monitoring users and system activity; auditing system configuration for vulnerabilities and misconfiguration; assessing the integrity of critical system and data files; identifying known attack patterns in system activity; recognizing abnormal activity through statistical analysis; managing audit trails and highlighting user violations of policy; correcting system configuration errors; and installing and operating traps to record information.

iii. Authentication and Access Control

24. Authentication and access control mechanisms prevent unauthorized access to computers, applications, services, and data.

25. To authenticate themselves, users provide a combination of information that tells the system who they are (identity) and information that proves that identity (proof). Usernames and passwords are commonly used to authenticate users. When authenticating, a user enters her username to identify herself to the authentication system, and her password to prove her identity. Some authentication mechanisms may require multiple forms of proof. For example, a user may be required to provide a password (what she knows), and proof of using something she possesses, such as a biometric (finger print, iris scan, etc.) or token. An authentication mechanism that requires two forms of proof is called two-factor authentication, and it is used as part of a defense in depth strategy (see Section III.B below) to reduce the risk of compromise. Remote login and access to highly sensitive data are scenarios for which either two-factor or multi-factor authentication is often used.

26. Access control mechanisms restrict a user's access to computers, services, applications, or data. An access control mechanism enforces policies that specify the resources that users may access. A user's role, security clearance, etc., may be used to identify the resources to which that user has access.

B. Defense in Depth

27. The most effective way to secure a network and its computers is by using multiple security measures to provide defense in depth. In such an approach, the network is viewed as a system with multiple layers, and security mechanisms are deployed at each layer to reduce the overall likelihood that an attack will succeed. The basic idea is not to rely on just one security

measure. Practicing defense in depth reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple defenses. To generally illustrate the benefit of defense in depth, assume that an attacker has a 50% chance of penetrating each defense mechanism. If there are three layers of protection, the probability of gaining unauthorized access to a resource at the innermost layer is $(1/2)^3 = 1/8$.

28. To illustrate the concept of network layers and defense in depth, consider Figure 1 above. In this simple network, the layers are: the router that connects the LAN to the Internet; the computers on the LAN; and applications on each computer on the LAN. Defense in depth on this network would require security policies and mechanisms to be specified and deployed at the router that connects the LAN to the Internet, at the workstations/servers, and at user accounts on those computers.

29. Continuing with the simple network in Figure 1, assume there is a risk that a company's employees will download and install on their computers applications they do not need to perform their jobs and that the company has a security policy prohibiting unauthorized applications. A simple prohibition that relies on employees following the policy does not provide defense in depth. A defense in depth strategy would prevent the employee from installing the application and/or limit the impact of an unauthorized application on the network. To achieve defense in depth, the company should use different security measures at different layers in the network, as follows:

a. **Internet Connection Layer:** At this layer, we cannot prevent software from being installed on a workstation or server, but we can restrict the type of traffic that flows into the network. Therefore, even if unauthorized software has been inadvertently installed on a workstation/server, mechanisms could be used to render the application

ineffective. Recall that port numbers map to specific applications, and that firewalls can be configured to restrict the types of application traffic that is allowed into the network, by dropping any data that contains an unauthorized port number. Thus, to illustrate the concept of defense in depth, a first line of defense to prevent use of unauthorized applications is to configure a firewall to close all ports at the gateway router except those that are used by authorized applications. Other mechanisms besides firewalls could be deployed at this layer as well, such as an IDS.[2]

b. **Workstation/Server Layer:** Even if a firewall were deployed at the gateway router, a second layer of security may be appropriate. The firewall at the gateway router may be misconfigured or not configured to discard all unauthorized traffic because the corresponding firewall policy would be hard to implement and manage. In these circumstances, a software firewall can be deployed at workstations and servers to further filter traffic that may have passed through the firewall at the gateway router. Because the firewall at a workstation or server is configured to protect that specific computer, the security settings can be more restrictive.

c. **User Account Layer:** Finally, in the simple network in Figure 1, user accounts for specific computers could be configured to so that system administrators can install software but ordinary users cannot.

30. As illustrated above, deploying security measures at different layers of a network enhances overall security by closing gaps in any one measure. In practice, achieving defense in

[2] A firewall and IDS could be used together to provide additional protection. If an IDS detects a violation, it could send a security alert to the system administration, indicating that unauthorized traffic is entering the network (i.e. traffic destined for an unauthorized application) and that firewall settings need to be updated to discard such traffic.

depth involves using layered security measures to address the many different risks and vulnerabilities a network may face.

C. Principles for Assessing and Securing a Network

31. There are seven principles that help to specify the policies and identify the mechanisms that are to be deployed at each layer of a defense in depth security strategy. These principles are listed and described below.

a. **Don't Keep What You Don't Need:** The first principle recognizes that maintaining sensitive information that is not needed creates an unnecessary risk.

b. **Patch:** A most basic principle is to Patch, meaning to apply updates to fix all known or reasonably foreseeable security vulnerabilities and flaws.

c. **Ports:** The third principle concerns Ports. As previously stated, applications communicate via ports. There are well-known ports for well-known applications. For example, a web server listens for incoming connections on Ports 80 and 443. All unused ports should be closed.

d. **Policies:** Policies are processes and procedures that are put in place to satisfy an organization's security requirements. Examples of policies would include the following:

- **Data Access** – Limit data access to persons with a need for the data.
- **Passwords** – Policies regarding passwords should contain rules about the following:
  - Acceptable minimum length.
  - Lifetime of a password.
    - The lifetime of a password is often related to the sensitivity of the information that the user accesses, the greater the sensitivity, the shorter the password's lifetime.
  - Password history.

- Passwords to avoid.
  - If you are a big sports fan, don't use a password that is related to your favorite team.
  - Avoid personal data such as spouse's name, children's name, pet's name, and birthdays.

- **Backups** – Backup data on a regular basis to be able to restore it because data is more valuable than the computer.
  - Encrypt backups.
  - Keep data in a secure location.
  - Limit access to backups.

e. **Protect:** Ensure that reasonable security software is employed, such as firewalls, anti-spyware, anti-virus, and IDS software, and authentication and access control. This list includes software that can be classified as either proactive or reactive. Proactive mechanisms attempt to prevent threats, while reactive mechanisms respond to threats that may have bypassed proactive mechanisms. Therefore, both types of mechanisms should be used to secure a system. Firewalls, authentication, and access control mechanisms try to block or prevent attacks. Anti-spyware, anti-virus, and IDS mechanisms attempt to detect the presence of malicious software or an attack while it is occurring.

f. **Probe:** Probing is a security audit that tests the state of a network. One type of probing is penetration testing, which searches the network for security flaws. Penetration testing includes scanning ports to verify that unused ports are closed or disabled. A thorough security probe would include a review of security policies, patching system, security logs, computers for unauthorized software, and any other processes, procedures, or information that may impact the security of a system.

g. **Physical:** There must be policies that govern the physical access to devices and data. Some examples of such policies include:

- Computer rooms must be locked.
- Server rooms must be locked with limited access.

IV. LabMD's Network During the Relevant Time Period

32. LabMD's network was small and simple. It included: computers LabMD provided to physician clients to use to place orders and retrieve results over the Internet; a small number of servers located at its business premises; and computers used by employees. In this section, I describe at a high level the network during the Relevant Time Period.

33. LabMD provided computers to physician clients. Through these computers, physician clients sent Personal Information over the Internet to LabMD. This information included names, addresses, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. In some instances, physician clients entered the information into the computer that LabMD had provided, one consumer at a time, and then sent the information to LabMD. In other instances, the LabMD computer in the physician's office retrieved Personal Information for all patients of the physician's practice from a database located on another computer in the physician's office and forwarded the information for all of those patients in bulk to LabMD, regardless whether LabMD performed testing for those patients.

34. The Personal Information LabMD received from physician clients typically was transmitted from physician clients to LabMD's network using a File Transfer Protocol (FTP) service LabMD installed on its network and the computers it provided to physician offices.

35. Regardless of whether Personal Information came as a bulk transfer or one consumer at a time, it was received by a server on LabMD's network (called Mapper), where it was processed (so that it could be used by applications LabMD used in is laboratory and billing department) and

then maintained on servers on the network. The laboratory and billing applications also ran on servers on LabMD's network. In addition, LabMD maintained Personal information on desktop computers, such as the Finance/Billing Manager's computer.

36. After LabMD's laboratory and medical employees had provided the services ordered by physician clients, they added results to the Personal Information LabMD maintained on its network.

37. The evidence in the record shows that LabMD did not encrypt Personal Information while it was maintained on LabMD's network.

38. Physician clients typically retrieved the results of the services they ordered from LabMD through LabMD's web portal. In doing so, they accessed Personal Information stored on LabMD's network.

39. LabMD's network included a number of servers that hosted applications, including back-up, email, webserver, database, laboratory, and billing applications. Some of these servers hosted multiple applications and also stored Personal Information. For example, one server hosted billing and mail applications [3]

40. Employees in the laboratory and billing departments, and certain other employees, used their LabMD computers to access resources on LabMD's network, including applications that provided access to Personal Information maintained on the network. Some LabMD employees could remotely access LabMD's network, including Personal Information maintained on the network.

---

[3] See, for example, FTC-LABMD-00002 (CX0034).

41. Record evidence shows that in 2005 or 2006, LimeWire, a peer-to-peer (P2P) file-sharing program, was installed on a computer on LabMD's network. The computer was used by the Billing Manager.

42. At a high level, the software is called peer-to-peer because users use it to search for and retrieve files directly from the computers of others using the software instead of retrieving files from a central server. To do this, the software allows users to designate or place files they will share in a folder (Sharing Folder). Using the software, a user can search the Sharing Folders of other users for files of interest. P2P programs have been widely available since 1999, and have been, and are, used by millions of users to share music, video, and other types of files.

43. Record evidence, including a screenshot of the Sharing Folder on the Billing Manager's computer taken in May 2008, shows that hundreds of files were in the Sharing Folder on the Billing Manager's computer.[4] Among these files was an insurance aging file (called the 1,718 File) that contained Personal Information about more than 9,300 people.[5] Copies of the 1,718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom.[6]

44. The risk of inadvertently sharing files with sensitive information using P2P software and the difficulty of undoing sharing are well known. After a file has been shared, the copy is out of the control of the original source and can be shared again from its new location to any number of other computers running the software. Searching for the file might not find all of the copies

---

[4] See FTC-LABMD-3755 (CX0152).

[5] See FTC-LABMD-3755 (CX0152); Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008)

[6] See Robert Boback, November 21, 2013 Deposition Transcript, pp. 50-53; TIVERSA-FTC_RESPONSE-000001 through TIVERSA-FTC_RESPONSE-006876 (CX0008-CX0011); TIVERSA-FTC_RESPONSE-006882 (CX0019).

because, for example, a computer with a copy might be turned off when the search occurs. Security professionals and others have warned about this risk since at least 2005.

V. Scope of Opinions

45. Complaint Counsel has asked me to assess whether LabMD provided reasonable and appropriate security for Personal Information within its computer network. Specifically, I was asked to analyze the record evidence relating to the following paragraphs of the FTC's complaint:

a. Paragraph 10: "At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

- (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;
- (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;
- (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- (d) did not adequately train employees to safeguard personal information;
- (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;
- (f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely

that the systems would be updated to address newly discovered vulnerabilities; and

- (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks."

b. Paragraph 11: "Respondent could have corrected its security failures at relatively low cost using readily available security measures."

VI. Materials Considered in Forming Opinions

46. A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B. Those materials include: transcripts and exhibits from investigational hearings and depositions of LabMD, its current and former employees, and third parties; documents and correspondence provided to Complaint Counsel by LabMD and third parties in connection with the pre-complaint investigation or this litigation; and industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners. I also have relied upon my education and experience in reaching my opinions.

47. I am continuing to review material obtained by Complaint Counsel through discovery in this litigation. LabMD produced to Complaint Counsel more than 11,500 pages of documents between February 25 and March 4, 2014, and Complaint Counsel has informed me that depositions are noticed to be taken after March 18, 2014. I reserve the right to revise or supplement my opinions based upon my continued review of the documents recently produced by LabMD, information learned during depositions conducted after the submission of this report,

or any other new information relevant to this litigation that comes to my attention after the submission of this report.

48. As I noted in Paragraph 4, above, my overall conclusion and the specific opinions that support that conclusion cover the Relevant Time Period, which is January 2005 through July 2010. From my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.

VII. Summary of Opinions

49. Based on my review of the materials described in Section VI, above, and my experience described in Section II, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures. In reaching this conclusion, I have taken into account the amount and nature of the data maintained within LabMD's network, LabMD's network and security practices, risks and vulnerabilities on LabMD's network, and the cost of remediating those risks and vulnerabilities. Record evidence shows that LabMD maintains Personal Information about more than 750,000 consumers.[7] For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information.

50. In Section VIII, below, I present my specific opinions that support my overall conclusion. In each subpart of Section VIII, below, I present my specific opinions regarding whether LabMD

[7] See LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23. For most of those consumers, that information includes: Social Security numbers, insurance information, and medical diagnosis codes. See Tiversa-FTC_Response-000001 through Tiversa-FTC_Response-001719 (CX0008).

could have corrected its security failings at relatively low cost using readily available security measures, which relate to Paragraph 11 of the Complaint.

VIII. Opinions

A. Comprehensive Information Security Program – Complaint ¶ 10(a)

51. Complaint Counsel has asked me to provide an opinion on whether LabMD developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information. My opinion is organized as follows: (1) an explanation of the contents of a comprehensive information security program; (2) my opinion, including some examples of key evidence supporting those opinions.

52. A comprehensive information security program is a plan that sets out an organization's security goals, the written policies that would satisfy those goals, the mechanisms that would be used to enforce the written policies, and how those mechanisms would be used to enforce the written policies. The best practices for developing a comprehensive information security program would include the seven principles that I discuss in Paragraph 31, above: don't keep what you don't need, patch, ports, policies, protect, probe and physical.

53. A comprehensive information security program should be in writing to provide guidance to those who are implementing the plan and those who receive training through the plan. It also should be in writing to record the organization's current security goals and practices to facilitate changes to those goals and practices as security threats continually evolve and, because turnover is inevitable, to communicate the security goals and practices of the organization to future employees.

54. An organization's comprehensive information security program should specify confidentiality, integrity, and availability goals, and related policies and mechanisms.

55. A confidentiality goal/policy ensures that only authorized individuals are able to access data. Encryption and access controls are mechanisms that can be used to enforce confidentiality policies. Encryption mechanisms are used to protect stored data and data that is being transmitted between parties, but encryption alone doesn't prevent unauthorized individuals from gaining access to the data. If I encrypt the data and distribute the encryption key to everyone, the encryption procedure is ineffective. Therefore, in addition to encrypting the data, an organization should specify under which conditions should data be accessed and which employees should be allowed to access the data. Role-based access control policies have been often used by organizations to differentiate the data access of employees. In such policies, employees are assigned data access rights based on the job that they are required to perform.

56. An integrity goal/policy ensures that data is not inadvertently changed or lost. Mechanisms that enforce an integrity policy ensure that any unauthorized changes to a system and its data can be detected. For example, cryptographic hash functions may be used to detect unauthorized changes to stored data (i.e. software executables, patient records) and transmitted data. A cryptographic hash function takes data input of any size and computes a fixed-size number called a hash value that is unique to the data and can be used as the digital fingerprint for the data. Thus, changes in a file's hash value indicates that the file has been changed. Integrity-based software scanners can be configured to detect newly added software and/or changes to existing application executables. Any new software that has been installed on a computer may indicate an unauthorized installation, while changes to existing executables may denote that malware has been embedded in an application.

57. An availability goal/policy specifies processes to ensure that the computing system (i.e. hardware, software, and network), and data are accessible, even in the presence of natural disasters or malicious attempts to compromise the system.

58. Achieving confidentiality, integrity, and availability goals may incorporate the use of a variety of security mechanisms, including firewalls, intrusion detection systems, integrity scanners, anti-virus scanners, backups, logging, authentication, physical security, access control, risk assessment, and remediation, etc.

59. While security goals, policies and mechanisms are key components of any security plan, the success of any defense-in-depth based information security program will be limited when the users and managers of the computing system are not properly trained. Therefore any comprehensive security plan should also include training procedures for non-IT and IT employees. This training should ensure that employees understand the security goals and policies and how to use any mechanisms that are to be used to secure the system. In addition, IT staff should receive training on specific mechanisms to mitigate risks and on evolving threats. I discuss the training component of a comprehensive information security program in more detail in Section VIII.D, below.

60. Securing electronic health data is a topic that has been explored by many national experts for years, which has resulted in the creation of best practices and guidelines for securing this information. Examples of comprehensive information security programs concerning electronic health data have been available online at no cost from various sources since as early as 1997, including, for example, the National Research Council (NRC), the National Institute of Standards and Technology (NIST), and the Health Insurance Portability and Accountability Act

(HIPAA) Security Rule.[8] These comprehensive security programs include guidelines for ensuring the confidentiality, integrity, and availability of data, including mechanisms for authenticating individual users, employing access control mechanisms to restrict access based on an individual's role, limiting a user's ability to install software, assessing risks and vulnerabilities, encrypting stored data and data in transit, logging access to data and system components, ensuring system and data integrity, protecting network gateways, maintaining up-to-date software, etc.

61. Based on my review of evidence from the record, I have formed the opinion that LabMD did not develop, implement or maintain a comprehensive information security program to protect consumers' Personal Information. Record evidence shows that:

a. From 2005 to 2010, LabMD had no written information security program.[9] During the Relevant Time Period, LabMD employees received an employee handbook, but this document did not address the practices covered by a comprehensive security program. For example, the handbook states that LabMD has taken specific measures to comply with HIPAA but does not explain those measures.[10]

---

[8] See, for example, National Research Council, For the Record: Protecting Electronic Health Information (1997), at http://www.nap.edu/openbook.php?record_id=5595&page=R1; Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf; SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343; and Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[9] LabMD's Policy Manual, FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006) and LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual, FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007), were written in 2010. See, for example, John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 78-79, 91-92.

[10] See FTC-LABMD-003531 through FTC-LABMD-003553 (CX0001), p. 6; FTC-LABMD-003554 through FTC-LABMD-003575 (CX0002), p. 6.

b. Although LabMD contends that the policies set forth in LabMD's Policy Manual[11] were in place in 2007 and 2008, there is no documentation demonstrating that those policies were in place, and if they were in place, at least some of those policies were not being enforced. For example:

- LabMD contends that it adopted policies in 2002 to identify and remove unauthorized software that had been installed on employee computers and to configure firewalls on employee computers to block incoming connection requests. If these policies had been implemented, unauthorized software would have been detected and removed from employee computers, and computers located outside LabMD's network would not be able to initiate communications with computers inside the network. As discussed in Paragraphs 41-43, above, LimeWire, an unauthorized P2P file sharing program, was installed on the Billing Manager's computer in 2005 or 2006 and used to share files. LabMD's processes did not detect the software or prevent its use. LabMD removed the software in May, 2008, approximately two to three years from the date of installation, after being informed that the 1,718 File was found on a P2P network.

- In 2007 and 2008, when LabMD contends that the policies in its Policy Manual were in place, LabMD did not provide the encryption tools listed in its policy or provide staff with training on how to secure sensitive information included in emails or attachments.[12]

c. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual,[13] both of which were written in 2010, are not sufficiently comprehensive. For example, they lack specific policies that describe how Personal Information is protected during transmission between the physician offices and LabMD, and whether sensitive information is to be stored in an encrypted format.

---

[11] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); John Boyle February 5, 2013, Investigational Hearing Transcript, pp. 91-92.

[12] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 277-278; Alison Simmons May 2, 2013 Investigational Hearing Transcript, p. 163.

[13] See FTC-LABMD-003141 through FTC-LabMD-003162 (CX0006); FTC-LABMD-003590-3621 (CX0007).

- LabMD relied on the Secure Socket Layer (SSL) Protocol and HTTPS to encrypt communications and secure its web-based applications.[14] Record evidence shows that LabMD's servers allowed the use of SSL version 2.0, which had known security flaws.[15]

62. LabMD could have developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information at relatively low cost.[16]

B. Risk Assessment – Complaint ¶ 10(b)

63. Complaint Counsel has asked me to provide an opinion as to whether LabMD used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network, which is often called "risk assessment" in the IT field. My opinion is organized into several parts: (1) an explanation of why risk assessment is important; (2) a discussion of the mechanisms and protocols IT practitioners use to assess risks; and (3) my opinion, including some examples of key evidence supporting those opinions.

64. The relationship between risk assessments and reasonable security is very well known among IT practitioners, and frameworks for conducting risk assessments are widely available from many sources. When an assessment is inadequate or incomplete, network administrators and users may not know which risks or vulnerabilities they face and thus the security measures they should consider implementing. To IT practitioners, risk assessments are the foundation for choosing security measures that are reasonable and appropriate under their circumstances. It is an essential component of defense in depth.

65. IT practitioners use a variety of measures and techniques, to assess and remediate risks. These include antivirus applications, firewalls, various types of vulnerability scans, intrusion

---

[14] SSL is the protocol that ensures that data is encrypted for HTTPS.

[15] This vulnerability is discussed in Paragraph 100, below.

[16] See, for example, footnote 8, above, and the accompanying text.

detection systems, penetration tests, file integrity monitoring, and other measures. Typically, each mechanism can only assess the exposure to a particular type of risk or vulnerability. Antivirus applications, for example, can assess the incidence of viruses on a network, but not the installation of unauthorized applications on the network. Logs from firewalls, for example, can be reviewed to identify the application and host targets of unauthorized attempts to access the network, but traditional firewalls are designed to block specific types of traffic, not detect intrusions and attacks. An IDS can be used to detect attacks and alert the IT staff that firewall settings should be reconfigured. External vulnerability scans, which are conducted from outside the network, can, for example, assess the incidence of vulnerabilities in an application inside the network, but not the incidence of viruses. File integrity monitoring can identify changes in critical files that may indicate malware has been installed on the network, but does not identify or remove the malware. No one mechanism can assess the exposure to all the risks and vulnerabilities a network may face. An appropriate risk assessment process usually requires the use of a number of mechanisms.

66. Network administrators usually have a number of options to choose from in each mechanism category. For example, there are a number of branded antivirus applications, and within a brand there often are versions that differ in cost, the types of functions they can perform, and other aspects of performance. Properly used and reviewed, these mechanisms provide network administrators with essential information about risks and vulnerabilities they face. Having options provides companies with flexibility, so that they can balance the effectiveness of a mechanism, the sensitivity of the business and consumer information the assessment concerns, and the mechanism's cost.

67. Based on my review of the evidence from the record, I have formed the opinion that LabMD did not use an appropriate set of readily available measures to assess risks and vulnerabilities to the Personal Information within its computer network during the Relevant Time Period.

68. Record evidence shows that, prior to 2010, LabMD used antivirus applications, firewalls, and manual computer inspections to assess risks within the network. These mechanisms were not sufficient to identify or assess risks and vulnerabilities to the Personal Information maintained on LabMD's computer network.

a. As I discussed in Paragraph 65, above, antivirus applications can assess the incidences of viruses on a network but cannot assess the installation of unauthorized applications on the network. The evidence shows that at times, LabMD did not effectively manage its antivirus applications, or used applications that were out of date or had limited risk assessment functionality. For example, at some points, the antivirus application LabMD used on critical servers would not scan for viruses,[17] and thus could not identify risks to the servers. LabMD continued to use the same antivirus application after the vendor stopped providing updated virus definitions needed to identify newly discovered risks. On employee workstations, LabMD at times used antivirus applications that provided only limited risk assessment functionality, at least until late 2006. These applications could not be centrally managed by a network administrator; which meant that to be effective, individual employees had to update the virus definitions on their

[17] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

computers and report warnings to LabMD's IT Department. Even after it implemented a more capable antivirus application, LabMD did not install it on all its equipment.[18]

b. The firewall product that LabMD used until 2010 had very limited risk assessment capabilities. It could only log a few days of network traffic, which LabMD only reviewed to troubleshoot a performance problem, such as a user complaint that he or she could not connect to a website.[19] The firewall product also could not monitor traffic.[20] IT practitioners use traffic monitoring to, for example, determine if sensitive consumer information is being exported from their networks. LabMD could have used the freely available mechanism, Wireshark, to do packet level analysis to provide information to use to determine if Personal Information left the network without authorization.

c. Evidence in the record shows that, through at least mid-2008, LabMD conducted manual computer inspections only in response to a physician or employee reporting that a computer had malfunctioned.[21] Even when conducted on a regular basis, manual computer inspections can never be exhaustive because vulnerabilities and risks can exist anywhere in a computer, and human beings cannot inspect every one of those places. Even if they could, malicious software may, in some instances, mask its presence to avoid detection during a manual inspection, such as by altering the task manager application in Windows to prevent the malicious software's process from being displayed. For these reasons, IT practitioners should not rely on manual inspections and

---

[18] See, for example, Christopher Maire January 9, 2014 Deposition Transcript, p. 95; Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 150-151.

[19] See, for example, Allen Truett February 27, 2014, Deposition Transcript, pp. 68-69.

[20] See, for example, Allen Truett February 27, 2014, Deposition Transcript, p. 67.

[21] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 177-178; Alison Simmons Investigational Hearing Transcript, pp. 78-80, 85-86; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 50-52.

should also use automated mechanisms, such as IDS, file integrity monitoring, and penetration testing to assess risks and vulnerabilities on the network.

69. LabMD did not implement an IDS or file integrity monitoring,[22] and only began conducting penetration tests in May 2010. These tests were limited to external facing servers and did not test employee workstations and computers inside LabMD's network. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using these automated mechanisms.

70. A penetration test of all IP addresses on the network, for example, would have identified vulnerabilities like outdated software, security patches that had not been applied, administrative accounts with default settings, etc. IT practitioners use this information to address these vulnerabilities. Information from penetration tests also could have identified all open ports within the network and all computers that accepted connection requests. This information could have been used to re-configure firewalls to close unneeded ports and to deny connection requests for computers whose work purpose didn't require the servicing of such requests.

71. Several well-respected and freely available penetration test and network analysis mechanisms have been available since 1997. Examples include: nmap (www.nmap.org, released 1997), Nessus (free until 2008), and Wireshark (formerly Etheral, released 1998). Using these mechanisms, LabMD could have conducted vulnerability scans, or had vulnerability scans conducted for it, throughout the Relevant Time Period, and doing so would have allowed it to correct significant risks, including those I describe in Paragraph 72, below, much sooner. The

---

[22] LabMD could have implemented an IDS and file integrity monitoring during the Relevant Time Period at relatively low cost. For example, LabMD could have implemented SNORT, a well-respected and widely used IDS that has been freely available since 1998, and, as I explain in Paragraph 104 below, Stealth and OSSEC are examples of freely available file integrity monitoring products.

cost of having penetration tests is modest: the penetration test LabMD had performed in 2010 by ProviDyn, an IT service provider, cost $450.[23]

72. Evidence in the record shows that the external vulnerability scans conducted in 2010 identified a number of well-known and significant risks and vulnerabilities on LabMD's network, including some that had been known to IT practitioners for years. For example, ProviDyn's April 2010 external vulnerability scan report identified a Level 5 anonymous FTP problem. This problem was first reported by the security community on July 14, 1993, 17 years before ProviDyn found it on LabMD's Mapper server.

73. Under the IT industry standardized classification system ProviDyn used, a Level 5 risk is an Urgent Risk and requires immediate remediation.[24]

74. The process for choosing reasonable and appropriate measures to address risks discovered through risk assessment is well-known and understood among IT practitioners and businesses. Guidelines on how to select reasonable and appropriate security measures have been freely available for years. NIST, for example, published a standard that explained the process in 2002.[25] In 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central

---

[23] See, for example, FTC-LABMD-003732 through FTC-LABMD-003736 (CX0044); FTC-LABMD-005254 through FTC-LABMD-005258.

[24] The risk classifications ProviDyn used are the classifications in the PCI Data Security Standard, which are derived from the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards (NIST). See PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1 (September 2006). In this classification, there are 5 levels: Urgent Risk (5), Critical Risk (4), High Risk (3), Medium Risk (2), and Low Risk (1). Level 5 (Urgent Risk) Vulnerabilities provide remote intruders with remote root/administrative capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers with full file-system read and write capabilities, remote execution of commands as an administrative user.

[25] See NIST Risk Management Guide for Information Technology Systems SP-800-30 (July 2002), at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

principles of NIST SP 800-30 in explaining how to perform the risk analysis and risk management required by the HIPAA Security Rule.[26]

75. IT practitioners have used these concepts to identify security measures that are reasonable and appropriate under various circumstances for years. The basic idea is to balance the severity of a risk and the harm that will result if the risk is exploited against the cost of a measure that remediates the risk. The more sensitive the Personal Information maintained within the network, the greater the need for enhanced security measures,

76. Consider the anonymous FTP problem set out in Paragraph 72, above: users are anonymous because no password is needed to log into the FTP service. It is an urgent risk to an application that LabMD used to transmit large amounts of Personal Information. Thus, the risk is high and the harm that would result if the risk were exploited is also high. The cost of remediating it is low, involving only IT-employee time to disallow anonymous log-ins. As a result, it would be reasonable and appropriate under these circumstances to disallow anonymous log-ins. The point of conducting appropriate risk assessments is to identify risks early, so that they can be remediated.

77. LabMD could have used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network at relatively low cost.[27]

C. Access to Information Not Needed to Perform Jobs – Complaint ¶10(c)

78. Complaint Counsel has asked me to provide opinions as to (1) whether LabMD maintained more Personal Information than necessary on its network and (2) whether LabMD

---

[26] See U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

[27] See, for example, Paragraph 71, above.

used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs. My opinion is organized as follows: (1) an explanation of why it is important for an organization to not maintain more Personal Information than necessary on its network; (2) my opinion concerning whether LabMD maintained more Personal Information than necessary on its network, including some examples of key evidence supporting those opinions; (3) an explanation of why limiting access to Personal Information is important; (4) a discussion of the mechanisms IT practitioners use to limit access to information maintained within a network; and (5) my opinion concerning whether LabMD used adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs, including some of the evidence I considered.

i. Whether LabMD Maintained More Personal Information than Necessary

79. One of the principles of information security is for an organization to not maintain more information than it needs to conduct its business. This is important because, if an organization collects more data than is needed to conduct its business, it increases the scope of potential harm if the organization's network is compromised.

80. Based on my review of evidence from the record, I have formed the opinion that LabMD collected and maintained Personal Information about individuals for whom it has not performed testing (either directly or by outsourcing to another laboratory) and therefore did not use adequate measures to prevent employees from having access to Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD collected and maintained indefinitely Personal Information about approximately 100,000 consumers for whom it never performed testing (either directly or by outsourcing to another laboratory) and that

LabMD did not need to maintain Personal Information about those consumers in order to conduct its business.[28]

b. LabMD could have purged the data that it collected from consumers for whom it did not perform testing (either directly or by outsourcing to another laboratory) through its database applications. Purging data from a network is the type of thing that IT practitioners did regularly throughout the Relevant Time Period. Correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

ii. Whether LabMD Used Adequate Measures to Prevent Employees from Accessing Personal Information Not Needed to Perform Jobs

81. By not limiting access to data, an organization increases the likelihood that sensitive data will be exposed outside of the organization by either a malicious insider or a compromised system. Insider threat is one of the major issues facing organizations. Though some insiders do not have malicious intent, some scenarios create the perfect storm for the leaking of sensitive, personal data, especially health data. For example, in recent years, there have been several highly publicized events where individuals with celebrity status had their personal health information exposed by an insider of the health care organization. While these events are publicized, there are numerous others that are not. Friends, family members, co-workers or acquaintances access the personal health records of an individual outside of the organizations' policy, thereby violating that individual's right to privacy. To address this problem an organization must specify policies and employ mechanisms that limit an employee's access to data based on that which is needed to perform their daily tasks. For example, a lab tech may need information that identifies

[28] LabMD's March 3, 2014 Responses to Complaint Counsel's Requests for Admission, ¶ 23; Michael Daugherty March 4, 2014 Deposition Transcript, pp. 198-199.

the patient, but may not need the patient's insurance information. Additionally, when an organization has information about a large number of people, it is not only necessary to limit the types of information that an employee within a specific role may access, but it is also important to limit the number individuals whose Personal Information the employee may access. Doing so reduces the impact of a malicious insider.

82. In addition to the insider threat, when data may be accessed by multiple parties, the likelihood that the data may be accessed from a computer that has been compromised also increases. This is especially the case for organizations that do not have a comprehensive information security plan, and have security practices that are at best reactive. In such cases, when data is downloaded to a compromised computer, vulnerabilities on that computer may expose the data to individuals outside of the organization.

83. A multi-pronged, defense in depth, approach must be used to effectively restrict access to data. The organization must first define roles for its employees and specify the types of data that are needed to complete the tasks that have been assigned to those roles. To enforce these roles, IT practitioners have long used role-based access control mechanisms to restrict access to sensitive data resources. These mechanisms should be employed to restrict access to data files and to applications that mediate access to the data.

84. Based on my review of evidence from the record, I have formed the opinion that LabMD did not use adequate measures to prevent employees from accessing Personal Information that was not needed to perform their jobs.

a. Record evidence shows that LabMD is unable to specify the types of Personal Information that each of its employees was permitted to access via LabMD's network and can specify only that its employees had "various levels of access" to various types of

Personal Information and that "all employees could gain knowledge of any Personal Information regarding Consumers to the extent it was necessary to the performance of their job duties."[29]

b. Because LabMD cannot specify the types of Personal Information that each of its employees was permitted to access via LabMD's network, I conclude that LabMD did not specify policies and employ mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs.

85. LabMD could have specified policies and implemented access control mechanisms to limit its employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs at relatively low cost. Operating systems and applications have access control mechanisms embedded in them. Therefore, correcting this issue would have required only the time of trained IT staff and could have been done at relatively low cost.

D. Information Security Training – Complaint ¶10(d)

86. Complaint Counsel has asked me to provide an opinion as to whether LabMD adequately trained employees to safeguard Personal Information. My opinion is organized as follows: (1) an explanation of the importance of training; and (2) my opinion, including some examples of key evidence supporting those opinions.

87. The user is the weakest link in any information security program. A flawless security mechanism can be rendered ineffective by an untrained user. For example, a username/password

[29] LabMD's February 20, 2014 and March 17, 2014 responses to Complaint Counsel's Interrogatory No. 2. See also, for example, March 10, 2014 Order on Complaint Counsel's Motion for Discovery Sanctions, p. 5.

authentication mechanism is only effective when users create strong passwords. Weak passwords that are short in length, contain dictionary words, contain the names of relatives, or favorite sports teams are more easily guessed than others. Therefore, an organization should train its employees on how to use any security mechanisms that require employee action or any security mechanisms that employees are not technically prevented from reconfiguring (such as disabling a firewall on a workstation without IT staff approval).

88. Employees also should receive periodic training on expected and acceptable use of computing facilities and current threats and best usage practices.

89. Since computer threats and vulnerabilities are always evolving, IT practitioners should receive periodic training on the most recent advances in protecting against such threats. Several nationally recognized organizations provide low-cost and free IT security training courses.[30]

90. I see no evidence in the record indicating that LabMD's non-IT employees received training on how to use security mechanisms or training on the consequences of reconfiguring security settings in applications and security mechanisms on their computers, such as enabling file-sharing, which I discuss in Section VIII.G, below.

91. Record evidence shows that LabMD did not adequately train employees to safeguard Personal Information or provide appropriate opportunities for its IT employees to receive formalized security related training about evolving threats and how to protect against them.[31] This resulted in gaps in their knowledge and a creation of security processes that were reactive, incomplete, ad hoc, and ineffective. For example, prior to 2010:

---

[30] For example, the Center for Information Security Awareness, formed in 2007, provides free security training for individuals and businesses with less than 25 employees. The SysAdmin Audit Network Security Institute (SANS) formed in 1989, provides free security training webcasts. Additional free training resources may be found at http://msisac.cisecurity.org/resources/videos/free-training.cfm. The Computer Emergency Response Team (CERT) at Carnegie Mellon University has e-learning courses for IT professionals for as low as $850.

[31] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 52-53, 60-61.

a. Penetration testing was never done;[32]

b. Software with known flaws was not updated on servers that contained Personal Information;[33]

c. Firewalls were disabled on servers that contained Personal Information;[34]

d. Servers executed software that was no longer supported by vendors, including operating system and antivirus software;[35]

e. There was no uniform policy requiring strong passwords or expiration of passwords;[36]

f. Personal Information was transmitted and stored in an unencrypted format;[37]

g. At least some employees were given administrative access accounts and were able to download and install software without restriction, etc.[38]

92. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost.[39]

E. Use of Authentication Related Security Measures – Complaint ¶10(e)

93. Complaint Counsel has asked me to provide an opinion as to whether LabMD required employees, or other users with remote access to the network, to use common authentication-

---

[32] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 92, 281-282.

[33] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[34] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 293-294.

[35] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274; FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035).

[36] See, for example, Robert Hyer December 13, 2013 Deposition Transcript, pp. 25-27, 45-46; Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 153-154; John Boyle February 5, 2013 Investigational Hearing Transcript, pp. 181-184.

[37] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 62-64, 302-304.

[38] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 172; Alison Simmons Investigational Hearing Transcript, pp. 37-39; Robert Hyer December 13, 2013 Deposition Transcript, pp. 27-29.

[39] See, for example, footnote 30, above, and the accompanying text.

related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication. My opinion is organized as follows: (1) an explanation of why using authentication-related security measures is important; (2) a discussion of common authentication-related security measures to limit access; and (3) my opinion, including some examples of key evidence supporting those opinions.

94. Organizations should use strong authentication mechanisms to control access to workstations. Usernames/passwords are one such mechanism, but the effectiveness of this mechanism depends on the strength of the passwords and how the passwords are stored and managed. An organization should specify policies on how to create strong passwords. For example, password policies should specify acceptable length, required characters (numbers, case, symbols), lifetime, password history, passwords to avoid, etc. To enforce these policies: password management should be centralized; passwords should not be stored in clear text; and a cryptographic hash should be applied to the password before it is stored.

95. Based on my review of evidence from the record, I have formed the opinion that LabMD did not require employees or other users with remote access to its network, to use common, effective authentication-related security measures.

a. Record evidence shows that LabMD did not provide specific strong password policies or enforcement mechanisms to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network, either on site or remotely. For example:

- LabMD billing employee Sandra Brown testified that she used the same username, sbrown, and password, labmd, to access her LabMD computer on site and remotely from 2006 to 2013.[40]

---

[40] See Sandra Brown January 11, 2014 Deposition Transcript, p. 13.

- LabMD created weak passwords for the nurses' user accounts that were created on the computers that it placed in its physician clients' offices. The typical password included the nurse's initials.[41]

- Although the Windows operating systems that LabMD used provided a centralized scheme to manage passwords, LabMD did not use that functionality.[42]

- Requiring two-factor authentication for remote users would have implemented a defense in depth strategy and could have compensated for LabMD's failure to require the use of strong passwords. LabMD did not use two-factor authentication.[43]

b. Record evidence shows that between at least October 2006 and June 2009, passwords required for access to Personal Information were shared by multiple LabMD employees.[44]

96. LabMD could have easily implemented strong authentication-related security measures at low cost.

F. Maintenance and Updating of Operating Systems– Complaint ¶10(f)

97. Complaint Counsel has asked me to provide an opinion as to whether LabMD maintained and updated operating systems of computers and other devices on its network. My opinion is organized as follows: (1) an explanation of the risks of using outdated software; and (2) my opinion, including some examples of key evidence supporting those opinions.

---

[41] See, for example, Alison Simmons May 2, 2013 Investigational Hearing Transcript, pp. 46-48; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 39-41.

[42] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 171-172; Robert Hyer December 13, 2013 Deposition Transcript, pp. 84-88.

[43] See, for example, Alison Simmons, May 2, 2013 Investigational Hearing Transcript, pp. 47, 144, 152, 156; Curt Kaloustian May 3, 2013, Investigational Hearing Transcript, pp. 254-258; Matthew Bureau January 10, 2014 Deposition Transcript, pp. 83-84; Lawrence Hudson January 13, 2014 Deposition Transcript, pp. 74-75, 89, 183; Letonya Randolph February 4, 2014 Deposition Transcript, pp. 38-41.

[44] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, p. 79; Robert Hyer December 13, 2013 Deposition Transcript, pp. 26-27, 45, 62, 74-75.

98. Researchers have found that experienced programmers introduce 1 bug per every 10 lines of code that they write.[45] Therefore, for a program like Windows Server 2003[46] that has 50 million lines of code, you can expect approximately 5 million software bugs to be introduced while the software is being developed. While many of the bugs will be detected and fixed during system testing, not all bugs will be identified before the product is shipped. In addition, code that was added to fix a problem may also introduce new bugs.

99. Hackers exploit software bugs to gain unauthorized access to computer resources and data. To limit these exploits, IT practitioners should connect to product notification systems and immediately apply remediation processes and updates for vulnerabilities that have been identified. These systems provided freely available notifications from vendors, CERT, OSVDB, NIST, and others throughout the Relevant Time Period.

100. Based on my review of evidence from the record, I have formed the opinion that through at least 2010, LabMD did not adequately maintain and update operating systems of computers and other devices on its network.

a. Record evidence shows that LabMD servers executed software that had vulnerabilities that had been identified and reported by the security and IT community several years prior to being detected on LabMD computers.[47] This time delay indicates that LabMD was neither knowledgeable of nor responsive to security alerts and software updates for the products that it used.

---

[45] See Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional 1995.

[46] LabMD used Windows Server 2003 on at least some of its servers in May 2010. See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

[47] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

b. Record evidence shows that LabMD did not apply software updates in accordance with the policies it claims were in place during the Relevant Time Period[48] and had no policy for updating the software on hardware devices such as firewalls and routers.

c. Record evidence shows that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft.[49] The support life-cycle for Windows NT 4.0 ended on June 30, 2004, and Microsoft retired public and technical support and security updates on December 31, 2004. In a Microsoft press release, Microsoft states "Microsoft is retiring support for these products because the technology is outdated and can expose customers to security risks. The company recommends that customers who are still running Windows NT 4.0 begin migrations to newer, more secure Microsoft operating system products as soon as possible."[50]

d. Record evidence shoes that the LabMD Labnet server was running a version of Veritas Backup software that was configured with the default administrative password. This vulnerability had a Level 5 (Urgent Risk) rating, which means that an attacker can compromise the entire host. This problem was detected in 2010, and the corresponding solution was available as early as August 15, 2005. The Veritas software on the Labnet server also contained a Level 4 (Critical) buffer overflow vulnerability that would allow an attacker to execute arbitrary code on the remote host.[51] This problem was also detected

---

[48] See, for example, FTC-LABMD-003475 through FTC-LABMD-003482 (CX0035); FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006); FTC-LABMD-003590 through FTC-LABMD-003621 (CX0007).

[49] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 271-274.

[50] "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.

[51] Level 4 risks are "Vulnerabilities expose highly sensitive information and provide hackers with remote user capabilities. Intruders have partial access to file system; for example, full read access without full write access."

in 2010, and the corresponding solution was made available by the vendor on July 11, 2007.

e. Record evidence shows that several LabMD servers were running Integrated Information Services (IIS) web servers that used an insecure version of the Secure Socket Layer protocol (SSL 2.0).[52] This vulnerability had a Level 3 (High Risk) rating, which means that it provided hackers with access to specific information on the host, including security settings.[53] The vulnerability was detected on LabMD servers in 2010. Microsoft provided instructions on how to disable SSL 2.0 as early as April 23, 2007. Microsoft released Windows Server 2008 along with IIS 7.0 on February 27, 2008 and recommended both as upgrades to address the SSL 2.0 flaw. Thus, remediation for the flaw was available for three years prior to the vulnerability being detected on LabMD's network by the ProviDyn scan.

101. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost.

G. Prevention and Detection of Unauthorized Access – Complaint ¶10(g)

102. Complaint Counsel has asked me to provide an opinion as to whether LabMD employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. My opinion is organized as follows: (1) an explanation of the available measures and how they could have been deployed to prevent or detect unauthorized access to

---

[52] See, for example, FTC-PVD-001038 through FTC-PVD-001079 (CX0070). SSL is the protocol that ensures that data is encrypted for https.

[53] Level 3 risks are "High Risk vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level vulnerabilities could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying)." FTC-PVD-001038 through FTC-PVD-001079 (CX0070).

Personal Information; and (2) my opinion, including some examples of key evidence supporting those opinions.

103. Since security threats and vulnerabilities are changing constantly, security mechanisms that prevent an attack can never be exhaustive. Therefore, a defense in depth strategy must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker and detect unauthorized access when an attack is successful. The process of detection enables the organization to identify and patch holes in its security system.

104. There are several proactive, measures that should be employed, as part of a defense in depth strategy, to prevent the unauthorized sharing of Personal Information with external entities, including:

a. Employees should be given non-administrative accounts on workstations, thereby preventing them from installing software. Windows includes the functionality to enforce this policy in its operating systems package. This is a cost free measure.

b. Backups of Personal Information should be stored on devices that are isolated from other employee activities. An employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, etc. Therefore, backups of Personal Information should not be stored on multi-purpose employee workstations. Enforcing such a policy could be cost-free, if the organization designated an existing device for storage purposes only.

c. Windows operating systems provide the functionality to allow users to create folders that are stored on their individual workstations that can be shared with others.[54]

---

[54] These folders are different from shared folders on a network server that are centrally managed by IT staff.

When a folder is shared, it allows others to view the files that are contained within the folder.

d. While shared folders facilitate document sharing within an organization, there are many opportunities to mis-configure the sharing settings, which may lead to the inadvertent sharing of sensitive information with unauthorized parties. Such misconfigurations may include: giving read/write permissions to unauthorized parties, including restricted files in the shared folders, not including password protection, etc. In addition to the risk of misconfigurations, file-sharing applications, like LimeWire, also present the contents of shared folders to other users of those applications as information that is available to be downloaded. Therefore, employees should not be permitted to create shared folders on their workstations. Enforcing a no-shared folders policy requires no additional software, and can be achieved by configuring folder settings to disallow sharing and periodic monitoring of those settings.

e. A firewall should be employed at the network gateway to block all unwanted traffic from entering the network. The gateway firewall could be configured to block traffic destined to all unauthorized applications, such as file-sharing applications, which in turn would prevent traffic for those applications from entering the network. This type of configuring would create a list of acceptable applications and was routinely done by IT practitioners throughout the Relevant Time Period.

f. In addition, all employee workstations should be configured to use a software firewall. On August 25, 2004, Microsoft released its Windows Firewall as part of Windows XP Service Pack 2. This software firewall could be configured to block all incoming connection requests to a workstation. This would prevent, for example, users of

file-sharing applications, like LimeWire, from establishing a successful connection with a workstation and downloading shared files. The Windows Firewall accompanied the operating system at no cost to the customer.

g. Properly configuring firewalls at the network gateway and on employee workstations implements a defense in depth strategy for network protection. This provides protection and the outer network layer and the inner workstation layer to provide more robust protection against unauthorized attempts to access the network infrastructure.

h. File Integrity Monitors (FIM) take an initial snapshot of the files that are stored on a computer and periodically monitor the system to determine whether any changes have occurred. Any change may indicate malicious activity and raises an alert notification, indicating further investigation is needed. A FIM can be used to determine the presence of unauthorized software on a system. There are both free and commercially available FIM products. Stealth[55] and OSSEC are examples of free products, and Tripwire is an example of a commercial product. These are the types of mechanisms that IT practitioners used regularly throughout the Relevant Time Period.

105. Based on my review of evidence from the record, I have formed the opinion that LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network.

a. Record evidence shows that LabMD actively stored backups of highly sensitive Personal Information on the Billing Manager's workstation.[56] At least one document

---

[55] "Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host," http://stealth.sourceforge.net/, accessed on March 17, 2014.

[56] See FTC-LABMD-003141 through FTC-LABMD-003162 (CX0006).

containing [a backup of] Personal Information was stored in a shared folder on the Billing Manager's workstation, which made it accessible to the unauthorized file-sharing application that had been previously installed on that computer.

b. As discussed in Paragraph 61, above, record evidence shows that LabMD did not detect and remove the file-sharing application, LimeWire, until 2008, two to three years after it had been installed.[57] Had LabMD used FIM products to periodically monitor the Billing Manager workstation during this two to three year period, it might have detected the LimeWire application by, for example, detecting its installation or detecting music files downloaded through LimeWire. FIM therefore would have strengthened a defense in depth approach.

c. Record evidence shows that LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network.[58]

106. LabMD could have employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network at relatively low cost.

---

[57] See, for example, July 16, 2010 Letter from P. Ellis to A. Sheer (FTC-LABMD-002495 through FTC-LABMD-002503).

[58] See, for example, Curt Kaloustian May 3, 2013 Investigational Hearing Transcript, pp. 98-103.

IX. Conclusion

107. Based on my review of the materials described in Section VI, above, my experience described in Section II, above, and the specific opinions presented in Section VIII, above, my overall conclusion is that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network throughout the Relevant Time Period of January 2005 through July 2010, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures.

Dated: March 18, 2014

Raquel Hill, Ph.D.

Appendix A

Home Address:
734 E. Moss Creek Drive
Bloomington, IN 47401
Phone(217)369-0105
hill raquel@gmail.com

School of Informatics and Computing
Indiana University
Bloomington, IN 47405
Phone (812) 856-5807
E-mail
ralhill@indiana.edu
www.cs.indiana.edu/~ralhill

Raquel Hill

Education

University of Illinois Urbana, IL
August 2003- July 2005 Post Doctoral Research Associate

Harvard University Cambridge, MA
November 2002 PhD Computer Science

- Dissertation: Sticky QoS: A Scalable Framework for Resource Reservations.
- Advisor: H.T. Kung

Georgia Institute of Technology Atlanta, GA
March 1993 MS Computer Science
June 1991 BS Computer Science with Honors

Professional Experience

Harvard University, Cambridge, MA, **Visiting Scholar,** School of Engineering and Applied Science, **Center for Research on Computation and Society,** 9/2013 – 5/2014

Indiana University, Bloomington, Indiana, **Associate Professor,** School of Informatics and Computing, 6/2012 –Present

Indiana University, Bloomington, Indiana, **Assistant Professor,** School of Informatics and Computing, 08-2005 – 6/2012

Indiana University, Bloomington, Indiana, **Research Fellow, Kinsey Institute,** 12/2010 – Present

Jackson State University, Jackson, Mississippi, **Adjunct Professor, Department of Computer Science,** 2010- Present

University of Illinois, Urbana, Illinois, **Post-Doctoral Research Associate,** Joint Appointment with Department of Computer Science and NCSA, 08/2003 – 07/2005

Georgia Institute of Technology Atlanta, GA, **Lecturer,** within the School Electrical and Computer Engineering, 11/2002 – 08/2003

Professional Experience

Harvard University, Cambridge, MA, **Research Assistant** 09/1998 – 09/2002

IBM Research , Hawthorne, NY, **Intern**, Summer 1999

Digital Equipment Corporation, Cambridge, MA, **Intern**, Summer 1997

Nortel Networks , RTP, NC, **Member of Scientific Staff**, 08/1993 – 08/1996

Hayes MicroComputer Products, Atlanta, GA, **Coop Student**, 03/1993-07/1993

Cray Research, Eagan, MA, **Intern**, Summer 1992

Cray Research, Chippewa Falls, WI, **Intern**, Summer 1991

IBM Corporation, Atlanta, GA, **Co-op Student**, 06/1987-9/1990

Grants

IBM Corporation, Equipment Grant – Cryptographic Co-processors
Equipment Value: $75,000.00 Date: 9/01/05 – Present

CACR: Privacy Enhanced Online Human Subjects Data Collection
Total Award Amount: $49,999.99 Date: 07/01/09 – 12/31/10
Role: PI Source of Support: IU

TC: Large: Collaborative Research: Anonymizing Textual Data and Its Impact on Utility
Total Award: $568,895 Date: 9/01/10 – 8/31/14
Role: PI Source of Support: NSF

FRSP: Childhood Obesity Studies with Secure Cloud Computing
Total Award: $36,500 Date: 9/1/11 – 12/31/13
Role: PI

Publications

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J. R. Heiman, L. Xiong, Evaluating Utility: Towards an Understanding of Sharing Differentially Private Behavioral Science Data, (Under Review).

Raquel Hill, Michael Hansen, Veer Singh, "Quantifying and Classifying Covert Channels on Android", *Journal of Mobile Networks and Applications*, Springer US. DOI. 10.1007/s11036-013-0482-7, (November 2013).

Publications

D. Hassan, R. Hill, "A Language-based Security Approach for Securing Map-Reduce Computations in the Cloud", To appear in the *Proceedings of the 6th IEEE/ACM International Conference on Utility and Cloud Computing*, December 9-12, 2013, Dresden, Germany.

R. Hill, M. Hansen, E. Janssen, S.A. Sanders, J.R. Heiman, L. Xiong, "An Empirical Analysis of a Differentially Private Social Science Dataset" In the *Proceedings of PETools: Workshop on Privacy Enhancing Tools, Held in Conjunction with the Privacy Enhancing Tools Symposium*, July 9, 2013, Bloomington, IN.

M. Hansen, R. Hill, S. Wimberly, Detecting Covert Communications on Android. In the *Proceedings of the 37th IEEE Conference on Local Computer Networks (LCN 2012)*, October 22-25, 2012, Clearwater, Florida.

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, J. Heiman, Uniqueness and How it Impacts Privacy in Health-Related Social Science Datasets, In the Proceedings of the *ACM International Health Informatics Symposium (IHI 2012)*, January 28-30, 2012, Miami Florida.

J. Harris, R. Hill, Static Trust: A Practical Framework for Trusted Networked Devices, In the *Proceedings of 44th Hawaii International Conference on System Sciences, Information Security and Cyber Crime Track*, (Kauai, HI, 2011), 10 pages, CDROM, IEEE Computer Society.

Al-Muhtadi, Raquel Hill and Sumayah AlRwais "Access Control using Threshold Cryptography for Ubiquitous Computing Environments". *Journal of King Saud University Computer and Information Sciences*, No. 2, Vol. 23, (July 2011).

R. Hill, J. Al-Muhtadi, W. Byrd, An Access Control Architecture for Distributing Trust in Pervasive Computing Environments, at the *6th IEEE/IFIP Symposium on Trusted Computing and Communications (TrustCom)*, In the *Proceedings of 8th IEEE/IFIP Conference on Embedded and Ubiquitous Computing*, (Hong Kong, China, 2010), 695-702.

J. Harris, R. Hill, Building a Trusted Image for Embedded Communications Systems, In the *Proceedings of 6th Annual Cyber Security and Information Intelligence Workshop*, (Oakridge, TN, 2010), ACM, NY, 65:4.

L. Wang, R. Hill, Trust Model for Open Resource Control Architecture, at *3rd IEEE International Symposium on Trust, Security and Privacy for Emerging Applications*, In the *Proceedings of 10th IEEE International Conference on Computer and Information Technology*, (Bradford, UK, 2010) 817-823.

Publications

Gilbert, J.E., MacDonald, J., Hill, R., Sanders, D., Mkpong-Ruffin, I., Cross, E.V., Rouse, K., McClendon, J., & Rogers, G. (2009) Prime III: Defense-in-Depth Approach to Electronic Voting. In the *Journal of Information Security and Privacy*, 2009

J. Al-Muhtadi, R. Hill, R. Campbell, D. Mickunas, Context and Location-Aware Encryption for Pervasive Computing Environments, In *Proceedings of the 4th IEEE Conference on Security in Pervasive Computing and Communications Workshops*, (Pisa, Italy, 2006), 283-289.

R. Hill, S. Myagmar, R. Campbell, Threat Analysis of GNU Software Radio, In the *Proceedings of the 6th World Wireless Congress*, (San Francisco, CA, 2005).

A. Lee, J. Boyer, C. Drexelius, P. Naldurg, R. Hill, R. Campbell, Supporting Dynamically Changing Authorizations in Pervasive Communication Systems, In the *Proceedings of the 2nd International Conference on Security in Pervasive Computing*, (Boppard, Germany, 2005), 134-150.

R. Hill, G. Sampemane, A. Ranganathan, R. Campbell, Towards a Framework for Automatically Satisfying Security Requirements, In the *Proceedings of Workshop on Specification and Automated Processing of Security Requirements in conjunction with the 19th IEEE International Conference on Automated Software Engineering*, (Linz Austria, 2004), 179-191.

R. Hill, J. Al-Muhtadi, R. Campbell, A. Kapadia, P. Naldurg, A. Ranganathan, A Middleware Architecture for Securing Ubiquitous Computing Cyber Infrastructures, *5th ACM/IFIP/USENIX International Middleware Conference*, October 2004, *in IEEE Distributed Systems Online*, 5,9 (September 2004), 1-.

R. Hill, H.T. Kung, A Diff-Serv enhanced Admission Control Scheme, In *Proceedings IEEE Global Telecommunications Conference*, (San Antonio, TX, 2001), 2549-2555.

Refereed Abstracts

A. C. Solomon, R. Hill, E. Janssen, S. Sanders, Privacy and De-Identification in High Dimensional Social Science Data Sets, *in the Proceedings of the 32nd Annual IEEE Symposium on Security and Privacy*, Oakland, California, May 22-25, 2011.

R. Hill, J. Camp, Communicating Risk within the GENI Infrastructure, *Workshop on GENI and Security*, University California, Davis, January 22-23, 2009.

R. Hill, J. Wang, K. Nahrstedt, Towards a Framework for Quantifying Non-Functional Requirements, *Grace Hopper Celebration of Women in Computing*, October 2004.

Refereed Abstracts

J. Al-Muhtadi, R. Hill, R. Campbell, A Privacy Preserving Overlay for Active Spaces, *Ubicomp Privacy Workshop in conjunction with the Sixth International Conference on Ubiquitous Computing*, Nottingham, England, September 2004.

Posters

R. Hill, A.C. Solomon, E. Janssen, S. Sanders, J. Heiman, Privacy and Uniqueness in High Dimensional Social Science and Sex Research Datasets, Presented at the 37th Annual Meeting of the International Academy of Sex Research, August 10-13, 2011, Los Angeles, California.

C. Boston, R. Hill, L. Moore, The Feasibility of Designing a Secure System to Prevent Surgical Errors Using RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

S. Camara, R. Hill, L. Moore, Understanding How RFID Technology Impacts Patient Privacy, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Johnson, R. Hill, L. Moore, Evaluating and Mitigating the Security Vulnerabilities of RFID Technology, *in the Proceedings of the CAARMS 15*, Houston, Texas, June 23-26, 2009.

R. Hill, J. Wang, K. Nahrstedt, Quantifying Non-Functional Requirements: A Process Oriented Approach, *in the Proceedings of the 12th IEEE International Requirements Engineering Conference*, Kyoto, Japan, September 2004.

Technical Reports

R. Hill, J. Al-Muhtadi, Building a Trusted Location Service for Pervasive Computing Environments, Technical Report, TR646, Computer Science, Indiana University, 2007.

Dissertation

R. Hill, Sticky QoS: A Scalable Framework for Resource Reservations, Doctoral Dissertation in Computer Science, Harvard University Division of Engineering and Applied Sciences, November 2002.

Symposiums

"Protecting Privacy in Sex Research: Challenges and solutions offered by new technologies and recommendations for the collection, protection and the sharing of multi-dimensional data", **Speakers:** Raquel Hill, School of Informatics and Computing, Indiana University, Ulf-Dietrich Reips, iScience, University of Deusto, Bilbao, Spain, Stephanie Sanders, Gender Studies, Indiana University, The 38th Annual Meeting of the International Academy of Sex Research, July 8-12, 2012, Lisbon, Portugal

Invited Talks

"Understanding the Risk of Re-Identification in Behavioral Science Data", Technology in Government Topics in Privacy Seminar, Data Privacy Lab, Harvard University, Cambridge, MA, November 4, 2013.

Invited Talks

"Evaluating the Utility of a Differentially Private Behavioral Science Dataset", Center for Research on Computation and Society (CRCS), Harvard University, Cambridge, MA, October 2, 2013.

"Balancing the Interests in Developing and Sharing Behavioral Science Data", Workshop on Integrating Approaches to Privacy Across the Research Lifecycle, Harvard University, Cambridge, MA, September 24-25, 2013.

"Kinsey Goes Digital", Kinsey Institute's Board of Trustees Meeting, Indiana University, Bloomington, IN, May 20, 2011.

"Integrity-Based Trust for Networked Communications Systems", Center for Applied Cyber-security Research, Indiana University, Bloomington, IN, December 2, 2010.

"From Kinsey to Anonymization: Approaches to Preserving the Privacy of Survey Participants", Department of Mathematics and Computer Science, Emory University, Atlanta, GA, November 19, 2010; Indiana University, Bloomington, IN, November 12,2010.

"PlugNPlay Trust for Embedded Communications Systems", Purdue University, CERIAS, October 14, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Characterizing Trustworthy Behavior of Email Servers", CAARMS 2009, Rice University, June 23-26, 2009; The Symposium on Computing at Minority Institutions, April 8-10, 2010, Jackson State University, Jackson MS.

"Hardware Enabled Access Control for Electronic Voting Systems", Rose Hulman, January 6, 2009; Jackson State University, February 26, 2009

"Hardware-enabled Access Control for the Prime III Voting System", Auburn University, June 16, 2008

"Understanding the Behaviors of Malicious Users of Pervasive Computing Environments", ARO/FSTC Workshop on Insider Attacks and Cyber Security, June 11-12, 2007, Arlington, Virginia.

"Trusting Your Security", Second Annual Network Security Workshop, Lehigh University, May 15-16, 2006

"Establishing a Trusted Computing Base for Software Defined Radio", Information Security Institute, Johns Hopkins University, February 2005, Baltimore, Maryland.

Invited Talks

"Towards a Framework for Automatically Satisfying Security Requirements", Department of Computer Science, Queens University, October 2004, Kingston, Ontario, Canada.

"Overlay QoS", Department of Computer Science, Auburn University, February 2004, Auburn, Alabama.
"Distributed Admissions Control for Sticky QoS", *Ninth Annual Conference for African-American Researchers in the Mathematical Sciences*, June 2003, West LaFayette, Indiana.

"Distributed Admissions Control for Sticky QoS". *Sixth Informs Telecommunications Conference*, March, 2002, Boca Raton, Florida.
Former Congressman Lee Hamilton, Professor Fred Cate, and Professor Raquel Hill, "Security and Privacy in a Cyberwar World: A conversation about Edward Snowden, the NSA and the outlook for reform", *Indiana Statewide IT Conference*, Indiana University, Bloomington, IN October, 29, 2013

Panels

R. Hill, "Building Trusting Systems: Trusting Your Security", *Workshop on Useable Security, co-located with 11th Conference on Financial Cryptography and Data Security*, February 2007, Lowlands, Scarborough, Trinidad/Tobago.

R. Hill, R. Campbell, "Understanding, Managing and Securing Ubiquitous Computing Environments", *Grace Hopper Celebration of Women in Computing*, October 2004, Chicago, Illinois.

C. Lester, R. Hill, M. Spencer, "Making Waves: Navigating the Transition from Graduate Student to Faculty Member", *Grace Hopper Celebration of Women in Computing*, San Diego, California, Oct. 4-6, 2006.

Teaching

University	Course	Semesters Taught
Indiana University	I230 Analytical Foundations of Security	Spring 2006, Fall 2007-2011
	CSCI P438 Introduction to Computer Networks	Fall 2009,2010,2012
	CSCI H343 Data Structures (Honors	Fall 2011,2012
	CSCI B649 Trusted Computing	Spring 2006-2011
	CSCI B649 Data Protection	Spring 2013
Georgia Institute of Technology	ECE 2030 Introduction to Computer Engineering	Spring 2003, Summer 2003

Professional Activities

Member of Technical Program Committee

- IEEE International Conference on Information Technology (ITCC) 2005, Pervasive Computing Track
- IEEE International Conference on Communications 2006: Network Security and Information Assurance Symposium
- Indiana Women in Computing Conference February 2006
- Workshop on Security, Privacy and Trust for Pervasive Computing Applications, September 2006, 2007, 2008, 2009, 2010
- Middleware Support for Pervasive Computing Workshop (PERWARE) at the 4th Conference on Pervasive Computing and Communications, March 2007, 2008, 2009
- IEEE International Conference on Computer Communications and Networks, (ICCCN'06), Network Security and Dependability Track, October 2006; (ICCCN'07), Pervasive Computing and Mobile Networking Track, August 2007.
- IFIP Sixth International Conference on Networking (Networking 2007, 2008),
- Fourth International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, March 17-20, 2008 (Tridentcom 2008)
- First International ICST Conference on Mobile Wireless Middleware, Operating Systems and Applications, February 13-15, 2008, (Mobileware 2008, 2009,2010

Member of Review Panel

- **National Science Foundation**
- **Department of Energy**

Appendix B

Appendix B
Materials Considered or Relied Upon

IH Transcripts and Exhibits	Bates Range
13.02.05 Boyle, John - Transcript	FTC-000001-FTC-000115
13.02.05 Boyle, John - Exhibits	FTC-000116-FTC-000376
13.02.06 Daugherty, Michael - Transcript	FTC-000377-FTC-000416
13.02.06 Daugherty, Michael - Exhibit #8	FTC-000225-FTC-000246
13.02.06 Daugherty, Michael - Exhibit #14	FTC-000283-FTC-000304
13.02.06 Daugherty, Michael - Exhibit #23	FTC-000417-FTC-000423
13.05.02 Simmons, Alison - Transcript	FTC-000424-FTC-000493
13.05.02 Simmons, Alison - Exhibits	FTC-000494-FTC-000512
13.05.03 Kaloustian, Curt - Transcript	FTC-000513-FTC-000638
13.05.03 Kaloustian, Curt - Exhibits	FTC-000639-FTC-000656

Deposition Transcripts and Exhibits

14.01.09 Maire, Chris
14.01.10 Bureau, Matt
14.01.11 Brown, Sandra
14.01.13 Hudson, Lawrence
14.01.17 Maxey, Jerry Southeast Urology Network Rule 3.33
14.01.24 Howard, Patrick
14.04.28 Boyle, John
14.02.04 Randolph, Letonya Midtown Urology Rule 3.33
14.02.05 Simmons, Alison
14.02.06 Martin, Jeff
14.02.07 Gilbreth, Patricia
14.02.14 Bradley, Brandon
14.02.17 Carmichael, Lou
14.03.04 Daugherty, Michael LabMD Rule 3.33
14.02.10 Daugherty, Michael
14.01.25 Garrett, Karalyn
14.02.21 Harris, Nicotra
14.02.11 Parr, Jennifer
14.01.31 Sandrev, Peter Cypress Communication Rule 3.33
14.02.27 Truett, Allen
13.12.02 Dooley, Jeremy
13.11.21 Boback, Robert Tiversa Rule 3.33
13.12.13 Hyer, Robert

Correspondence	Bates Range
10.02.24 Ellis Letter	FTC-LABMD-002506-FTC-LABMD-002520
10.06.04 Ellis Letter	FTC-LABMD-002523-FTC-LABMD-002524
10.07.16 Ellis Letter	FTC-LABMD-002495-FTC-LABMD-002503
10.07.16 Ellis Exhibits	FTC-LABMD-002505-FTC-LABMD-003131

10.08.30 Ellis Letter	FTC-LABMD-003132-FTC-LABMD-003137
10.08.30 Ellis Exhibits	FTC-LABMD-003138-FTC-LABMD-003270
11.05.16 Rosenfeld Letter	FTC-LABMD-003445-FTC-LABMD-003452
11.05.16 Rosenfeld Exhibits	FTC-LABMD-003453-FTC-LABMD-003628
11.05.31 Rosenfeld Letter	FTC-LABMD-003629-FTC-LABMD-003634
11.05.31 Rosenfeld Exhibits	FTC-LABMD-003635-FTC-LABMD-003748
11.07.22 Rosenfeld Email	FTC-LABMD-003749-FTC-LABMD-003750
11.07.22 Rosenfeld Email	FTC-LABMD-003756-FTC-LABMD-003756
11.07.22 Rosenfeld Email-Screenshots	FTC-LABMD-003757-FTC-LABMD-003761
11.12.21 CID to Daugherty and Responses	FTC-000417-FTC-000423
13.01.17 CID to Daugherty and Responses	NA
11.12.21 CID to LabMD and Responses	FTC-000116-FTC-000127
13.01.17 CID to LabMD and Reponses	NA

Documents Produced by LabMD

FTC-LABMD-000001-FTC-LABMD-000304
FTC-LABMD-000306-FTC-LABMD-000385
FTC-LABMD-000388-FTC-LABMD-000603
FTC-LABMD-000605-FTC-LABMD-000634
FTC-LABMD-000636-FTC-LABMD-000646
FTC-LABMD-000648-FTC-LABMD-000776
FTC-LABMD-003139-FTC-LABMD-003444
FTC-LABMD-003453-FTC-LABMD-003628
FTC-LABMD-003635-FTC-LABMD-003748
FTC-LABMD-003752-FTC-LABMD-003761
FTC-LABMD-003763-FTC-LABMD-004358
FTC-LABMD-004514-FTC-LABMD-004536
FTC-LABMD-004576-FTC-LABMD-004677
FTC-LABMD-004782-FTC-LABMD-004851
FTC-LABMD-004882-FTC-LABMD-004891
FTC-LABMD-004897-FTC-LABMD-004906
FTC-LABMD-004922-FTC-LABMD-004950
FTC-LABMD-004975-FTC-LABMD-005129
FTC-LABMD-005160-FTC-LABMD-005221
FTC-LABMD-005250-FTC-LABMD-005310
FTC-LABMD-005644-FTC-LABMD-005651
FTC-LABMD-005686-FTC-LABMD-006637
FTC-LABMD-006820-FTC-LABMD-006823
FTC-LABMD-006828-FTC-LABMD-006835
FTC-LABMD-007128-FTC-LABMD-007132
FTC-LABMD-007212-FTC-LABMD-007342
FTC-LABMD-007463-FTC-LABMD-007507
FTC-LABMD-007619-FTC-LABMD-007627
FTC-LABMD-007636-FTC-LABMD-007659
FTC-LABMD-007990-FTC-LABMD-007994
FTC-LABMD-008022-FTC-LABMD-008036

FTC-LABMD-008108-FTC-LABMD-008124
FTC-LABMD-008780-FTC-LABMD-008783
FTC-LABMD-009955-FTC-LABMD-009958
FTC-LABMD-009960-FTC-LABMD-010060
FTC-LABMD-010513-FTC-LABMD-010615
FTC-LABMD-010654-FTC-LABMD-010660
FTC-LABMD-011103-FTC-LABMD-011106
FTC-LABMD-011116-FTC-LABMD-011120
FTC-LABMD-011855-FTC-LABMD-011858
FTC-LABMD-012751-FTC-LABMD-012755
FTC-LABMD-013286-FTC-LABMD-013289
FTC-LABMD-013304-FTC-LABMD-013308
FTC-LABMD-013441-FTC-LABMD-013448
FTC-LABMD-014422-FTC-LABMD-014483
FTC-LABMD-014512-FTC-LABMD-014521
FTC-LABMD-014533-FTC-LABMD-014607
FTC-LABMD-014613-FTC-LABMD-014620
FTC-LABMD-014625-FTC-LABMD-014680
FTC-LABMD-014689-FTC-LABMD-014692
FTC-LABMD-014699-FTC-LABMD-014869
FTC-LABMD-014896-FTC-LABMD-014952
FTC-LABMD-014957-FTC-LABMD-015016
FTC-LABMD-015020-FTC-LABMD-015218
FTC-LABMD-015242-FTC-LABMD-015245
FTC-LABMD-015414-FTC-LABMD-015430
FTC-LABMD-015457-FTC-LABMD-015477
FTC-LABMD-015491-FTC-LABMD-015525
FTC-LABMD-015542-FTC-LABMD-015962
FTC-LABMD-015994-FTC-LABMD-016063
FTC-LABMD-016135-FTC-LABMD-016141
FTC-LABMD-016148-FTC-LABMD-016179

Documents Produced by Tiversa
TIVERSA-FTC RESPONSE-000001-006904

Documents Produced by Sacramento Police Department
FTC-SAC-000001-FTC-LABMD-000044

Documents Produced by the Privacy Institute
FTC-PRI-000001-FTC-PRI-001719

Documents Produced by Cypress Communication, LLC
FTC-CYP-000001-FTC-CYP-000001
FTC-CYP-0001656-FTC-CYP-0001725
FTC-CYP-0001729-FTC-CYP-0001733
FTC-CYP-0001735-FTC-CYP-0001757

FTC-CYP-0001759-FTC-CYP-0001763
FTC-CYP-0001765-FTC-CYP-0001772
FTC-CYP-0001784-FTC-CYP-0001811
FTC-CYP-0001881-FTC-CYP-0001896
FTC-CYP-0001898-FTC-CYP-0001899
FTC-CYP-0001954-FTC-CYP-0001968
FTC-CYP-0001973-FTC-CYP-0001976
FTC-CYP-0001983-FTC-CYP-0001984
FTC-CYP-0002008-FTC-CYP-0002009
FTC-CYP-0002109-FTC-CYP-0002109

Documents Produced by ProviDyn, Inc.
FTC-PVD-000001-FTC-PVD-001582

Documents Produced by TrendMicro
FTC-TRM-000001-FTC-TRM-000455

Web Content Considered or Relied Upon

- The Center for Information Security Awareness, http://www.cfisa.org/, last accessed March 18, 2014.
- Center for Information Technology, University of Groningen -- SSH-based Trust Enforcement Acquired through a Locally Trusted Host, http://stealth.sourceforge.net/, last accessed March 16, 2014.
- The Computer Emergency Response Team (CERT), https://www.cert.org/, last accessed March 18, 2014.
- The Computer Emergency Response Team (CERT) -- Anonymous FTP Activity (1997), http://www.cert.org/historical/advisories/CA-1993-10.cfm, last accessed March 18, 2014.
- Cisco -- Cisco 1841 Integrated Services Router, http://www.cisco.com/c/en/us/products/routers/1841-integrated-services-router-isr/index.html, last accessed March 16, 2014.
- Common Vulnerabilities and Exposures – The Standard for Information Security Vulnerability Names, http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0527, last accessed March 16, 2014.
- Federal Communications Commission -- Cybersecurity for Small Businesses, http://www.fcc.gov/cyberforsmallbiz, last accessed March 16, 2014.
- Microsoft Forum -- Disable SSL v2 in IIS6?, http://forums.iis.net/t/1131343.aspx, last accessed March 16, 2014.
- Microsoft News Center -- Microsoft Windows Server 2003 Is Available Worldwide Today (April 24, 2003), http://www.microsoft.com/en-us/news/press/2003/apr03/04-24windowsserver2003launchpr.aspx, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Security TechCenter – Security Guidance for IIS, http://technet.microsoft.com/en-us/library/dd450371.aspx, last accessed March 16, 2014.

- Microsoft Security TechCenter – Microsoft Security Advisory (2661254), http://technet.microsoft.com/en-us/security/advisory/2661254, last accessed March 16, 2014.
- Microsoft Security TechCenter – Microsoft Security Bulletin MS05-019 – Critical, http://technet.microsoft.com/en-us/security/bulletin/ms05-019, last accessed March 16, 2014.
- Microsoft Support – How to disable simple file sharing and how to set permissions on a shared folder in Windows XP, http://support.microsoft.com/kb/307874, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/?id=187498, last accessed March 16, 2014.
- Microsoft Support – How to install and use the IIS Lockdown Wizard, http://support.microsoft.com/kb/325864, last accessed March 16, 2014.
- Microsoft Support – Microsoft Security Advisory: Update for minimum certificate key length, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Microsoft Support, http://support.microsoft.com/kb/2661254, last accessed March 16, 2014.
- Multi-State Information Sharing & Analysis Center – Cyber Security Awareness Free Training and Webcasts, http://msisac.cisecurity.org/resources/videos/free-training.cfm, last accessed March 18, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2611, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3509, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2002-1717&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/search-results?query=cve-2005-0048&search_type=all&cves=on, last accessed March 16, 2014.
- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5969, last accessed March 16, 2014.

- National Vulnerability Database – National Cyber Awareness System, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1491, Last accessed March 16, 2014.
- Nmap.org – www.nmap.org, last accessed March 18, 2014.
- Open Source SECurity, http://www.ossec.net/, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/76, last accessed March 16, 2014.
- Open Source Vulnerability DataBase, http://osvdb.org/show/osvdb/193, last accessed March 16, 2014.
- Symantec - Symantec Backup Exec for Windows Server: PRC Interface Heap Overflow, Denial of Service, http://securityresponse.symantec.com/avcenter/security/Content/2007.07.11a.html, last accessed March 17, 2014.
- Symantec – VERITAS Backup Exec for Windows Servers, VERITAS Backup Exec for NetWare Servers, and NetBackup for NetWare Media Server Option Remote Agent Authentication Vulnerability, http://securityresponse.symantec.com/avcenter/security/Content/2005.08.12b.html, last accessed March 17, 2014.
- The SysAdmin Audit Network Security Institute (SANS) – Information Security Resources, http://www.sans.org/security-resources/, last accessed March 18, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/crck_vista.b, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/Malware.aspx?id=35451&name=CRCK_KEYGEN&language=au, last accessed March 16, 2014.
- TrendMicro – Threat Encyclopedia, http://about-threats.trendmicro.com/us/archive/grayware/CRCK_KEYGEN.AU, last accessed March 16, 2014.
- U.S. Department of Health and Human Services – Health Information Privacy: The Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/, last Accessed March 18, 2014.

Articles & Publications

- Espenschied, Jon, "Five free pen-testing tools" (May 27, 2008), http://www.computerworld.com/s/article/9087439/Five_free_pen_testing_tools, last accessed March 16, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.
- Halamka, John D., Szolovits, Peter, Rind, David, Safran, Charles, "A WWW Implementation of National Recommendations for Protecting Electronic Health Information" Journal of the American Medical Informatics, (Nov-Dec 1997), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC61263/, last accessed March 16, 2014.

- Houston, Peter, "Q&A: Support for Windows NT Server 4.0 Nears End; Exchange Server 5.5 to Follow in One Year," https://www.microsoft.com/en-us/news/features/2004/dec04/12-03ntsupport.aspx, last accessed March 17, 2014.
- Kelly, Allen, "Proper Management of SSL Certificates: Why it is Critical to Your Organization - Part II" (September 8, 2011), http://www.symantec.com/connect/blogs/proper-management-ssl-certificates-why-it-critical-your-organization-part-ii, last accessed March 16, 2014.
- Kissel, Richard, "Small Business Information Security: The Fundamentals" (October 2009), http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf, last accessed March 16, 2014.
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments" (September 18, 2012), http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf, last accessed March 18, 2014.
- PCI Security Standards Council "PCI Technical and Operational Requirements for Approved Scanning Vendors, Version 1.1" (September 2006), https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf, last accessed March 18, 2014.
- SANS Institute InfoSec Reading Room, "Understanding IIS Vulnerabilities - Fix Them!" (2001), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute InfoSec Reading Room, "Cryptanalysis of RSA: A Survey" (2003), http://www.sans.org/reading-room/whitepapers/webservers/understanding-iis-vulnerabilities-fix-them-296, last accessed March 16, 2014.
- SANS Institute InfoSec Reading Room, "The Many Facets of an Information Security Program" (2003), https://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343, last accessed March 18, 2014.
- Stoneburner, Gary, Goguen, Alice, Feringa, Alexis, "NIST Risk Management Guide for Information Technology Systems" NIST (July 2002), http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, last accessed March 18, 2014.
- U.S. Department of Health and Human Services, HIPAA Security Series, "6 Basics of Security Risk Analysis and Risk Management" (March 2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf, last accessed March 18, 2014.
- Wagner, David, Schneier, Bruce, "Analysis of the SSL 3.0 protocol," https://www.schneier.com/paper-ssl.pdf, last accessed March 16, 2014.
- Woody, Carol, Clinton, Larry, Internet Security Alliance, "Common Sense Guide to Cyber Security for Small Businesses" (March 2004), http://isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf, last accessed March 18, 2014.

Books

- Humphrey, Watts, "A Discipline for Software Engineering," Addison-Wesley Professional (1995).

- National Research Council, "For the Record: Protecting Electronic Health Information" Washington, DC: The National Academies Press (1997), http://www.nap.edu/openbook.php?record_id=5595&page=R1, last accessed March 16, 2014.

FTC Provided Documents

- 13.08.28 Complaint
- 14.02.19 Complaint Counsel's Requests for Admission to Respondent LabMD
- 14.02.20 Revised Answer to Complaint Counsel's Interrogatory 1 and 2
- 14.03.03 Respondent's Objections and Responses to Complaint Counsel's Requests for Admission
- 14.03.10 Order Granting In Part and Denying In Part Complaint Counsel's Motion for Discovery Sanctions
- 14.03.14 Order on Complaint Counsel's Motion for Discovery Responses
- 14.03.17 Respondent's Supplemental Response to Complaint Counsel's First Set of Interrogatories

Miscellaneous

- Federal Register, Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information" (October 15, 2002), http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt, last accessed March 18, 2014.
- Federal Register, Department of Health and Human Services, "Health Insurance Reform: Security Standards" (February 20, 2003), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf, last accessed March 16, 2014.

EXHIBIT 6

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Bureau of Consumer Protection
Division of Privacy and Identity Protection

January 27, 2014

VIA EMAIL AND COURIER

William A. Sherman, II
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Sherman:

This letter follows my letter of January 24, 2014. Enclosed is a disc containing Complaint Counsel's first production of documents responsive to LabMD, Inc.'s written discovery requests.

Specifically, the documents that appear at FTC-000894 through FTC-010652 are responsive to LabMD's Request for Production 10. The documents that appear at FTC-000894 through 002693 are responsive to LabMD's Interrogatory 18.

We will supplement this production with our continuing, rolling production of responsive, discoverable, non-privileged documents.

Please notify me when you have received the enclosed disc and I will then send you the encryption key.

Sincerely,

Laura Riposo VanDruff

Enclosure (1)

cc: Reed D. Rubinstein (*via* email)
Michael D. Pepson (*via* email)
Lorinda B. Harris (*via* email)
Hallee K. Morgan (*via* email)
Kent Huntington (*via* email)

Sunni Harris (*via* email)
Robyn Burrows (*via* email)

EXHIBIT 7

United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Bureau of Consumer Protection
Division of Privacy and Identity Protection

March 3, 2014

VIA EMAIL AND COURIER

William A. Sherman, II
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

Re: In the Matter of LabMD, Inc., FTC Docket No. 9357

Dear Mr. Sherman:

This letter follows my letters of January 24, 2014, January 27, 2014, and February 19, 2014. Enclosed is a disc containing Complaint Counsel's third production of documents responsive to LabMD, Inc.'s written discovery requests.

Specifically, the documents that appear at FTC-013803 to FTC-013853 are responsive to Request for Production 4 and Interrogatory 11. The documents that appear at FTC-012347 to FTC-012473 are responsive to Requests for Production 5. The documents that appear at FTC-010957 to FTC-012358, FTC-012474 to FTC-013766, and FTC-013854 to FTC-013898 are responsive to Request for Production 10. The documents that appear at FTC-011034 to FTC-011276, FTC-011305 to FTC-012112, FTC-012474 to FTC-012477, FTC-012491, FTC-012552 to FTC-012553, and FTC-013626 to FTC-013628 are responsive to Interrogatory 18.

Complaint Counsel also supplements its initial disclosures with the document located at FTC-013767 to FTC-013802.

Complaint Counsel has not collected or reviewed, other than in response to Respondent's discovery requests, any additional documents required to be produced by the Order Denying Respondent's Motion for a Rule 3.36 Subpoena (February 21, 2014). Nonetheless, documents that are relevant to the Complaint's allegation that "since 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks" appear in this production at FTC-011305 to FTC-011312, FTC-011841 to FTC-011874, FTC-012347 to FTC-012358, FTC-012478 to FTC-012490, FTC-012520 to FTC-012544, FTC-013626 to FTC-013628, FTC-013762 to FTC-013766, and FTC-013897 to FTC-013898.

Please note that certain documents have been marked "Confidential," pursuant to Paragraph 6 of the Protective Order. In particular, FTC-012363 is a native audio file and as such the contents could not be stamped "Confidential." The placeholder .TIF and the metadata, as well as the accompanying static document at FTC-012362, have been marked "Confidential" to indicate that the entire document is to be treated as confidential as described in Paragraphs 7 to 13 of the Protective Order. The document at FTC-013767 to FTC-013802 has also been marked confidential.

Please notify me when you have received the enclosed disc and I will then send you the encryption key.

Sincerely,

Laura Riposo VanDruff

Enclosure

cc: Reed D. Rubinstein (*via* email)
Michael D. Pepson (*via* email)
Lorinda B. Harris (*via* email)
Hallee K. Morgan (*via* email)
Kent Huntington (*via* email)
Sunni Harris (*via* email)
Robyn Burrows (*via* email)
Daniel Epstein (*via* email)

EXHIBIT 8

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of	)	FILE NO. 0423160
BJ'S WHOLESALE CLUB, INC., a corporation.	)	AGREEMENT CONTAINING CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of BJ's Wholesale Club, Inc., a Delaware corporation ("proposed respondent"). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between BJ's Wholesale Club, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent BJ's Wholesale Club, Inc. is a Delaware corporation with its principal office or place of business at One Mercer Road, Natick, Massachusetts 01760.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:

A. any further procedural steps;

B. the requirement that the Commission's decision contain a statement of findings of fact and conclusions of law; and

C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter

may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with

other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, "respondent" shall mean BJ's Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

D. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent's operations or business

arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an "Assessment") from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and

D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent's compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this seventeenth day of May, 2005

BJ's WHOLESALE CLUB, INC.

By: _____
BJ's WHOLESALE CLUB, INC.

_____
DAVID MEDINE
JAMES W. PRENDERGAST
Wilmer Cutler Pickering Hale and Dorr LLP
Counsel for respondent BJ's Wholesale Club, Inc.

FEDERAL TRADE COMMISSION

By: _____
ALAIN SHEER
Counsel for the Federal Trade Commission

APPROVED:

_____
JOEL WINSTON
Associate Director
Division of Financial Practices

_____
LYDIA B. PARNES
Director
Bureau of Consumer Protection

Alerta de la FTC para Consumidores

Uso Compartido de Archivos:
Cómo Evaluar los Riesgos

File-Sharing: Evaluate the Risks

Todos los días millones usuarios de computadoras comparten sus archivos en línea. Ya se trate de música, juegos o programas, el uso compartido de los archivos puede permitir que todas las personas compartan una gran cantidad de información. Usted simplemente descarga un programa software especial que conecta su computadora a una red informal de otras computadoras que operan con el mismo programa. Millones de usuarios pueden conectarse a la vez entre sí por medio de este programa, el cual frecuentemente es gratuito y fácilmente accesible.

¿No es verdad que parece alentador? Quizás, pero asegúrese de considerar cuáles serán los costos que tendrá que "pagar" a cambio. La Comisión Federal de Comercio (Federal Trade Commission, FTC), la agencia nacional de protección del consumidor, advierte que el uso compartido de archivos puede acarrear una cantidad de riesgos. Por ejemplo, cuando usted está conectado a programas de uso compartido, sin darse cuenta puede estar permitiéndoles a los demás que copien archivos privados que no tiene intención de compartir. Usted puede descargar material a su computadora que está protegido por las leyes de derechos de autoría y complicarse en problemas legales. Usted puede descargar un virus informático o facilitar que se violen las medidas de seguridad en línea; o tal vez descargar involuntariamente pornografía que está presentada bajo otros títulos.

Para proteger la información personal que tiene almacenada en su computadora, la FTC le recomienda que:

- Instale el programa de uso compartido de archivos con mucho cuidado. Si al instalar el programa usted no marca las configuraciones correctas, podría estar otorgando acceso no solamente a los archivos que desea compartir sino también a otra información grabada en el disco duro de su computadora, como por ejemplo sus declaraciones de impuestos, mensajes electrónicos, registros médicos, fotos y otros documentos personales.

- Tenga cuidado con los programas de espioaje (spyware). Algunos programas de uso compartido de archivos también instalan otros programas conocidos como spyware. Este programa de espionaje monitorea los hábitos de navegación del usuario y luego envía esos datos a terceros. Algunas veces, el usuario recibe anuncios basados en la información que el spyware ha recogido y diseminado. El spyware puede ser difícil de detectar y de eliminar de su computadora. Antes de usar un programa de uso compartido de archivos es probable que desee comprar un prorgama que pueda prevenir la descarga de este tipo de spyware o que lo ayude a detectarlo en el disco duro de su computadora.

- Apague su conexión. En algunas instancias el cierre de la ventana del programa de uso compartido de archivos no cierra realmente su conexión con la red. Esto permite que continúe activado el uso compartido de archivos y podría incrementar su riesgo de seguridad. Si usted tiene una conexión de Internet de alta velocidad o "banda ancha" (high-speed o broadband connection) usted sigue conectado al Internet a menos que apague su

computadora o desconecte su servicio de Internet. Este tipo de conexión permanente puede permitir que otros copien sus archivos en cualquier momento. Aún más, algunos programas de uso compartido de archivos se abren automáticamente cada vez que usted prende su computadora. Como medida preventiva, es posible que desee ajustar los controles de configuración del programa de uso compartido de archivos para evitar que se abra automáticamente.

- Utilice un programa software antivirus que sea efectivo y actualícelo regularmente. Los archivos que descarga pueden estar etiquetados incorrectamente y pueden ocultar un virus u otros contenidos indeseados. Utilice un programa antivirus para proteger su computadora contra los virus que pudieran provenir de los otros usuarios a través del programa de uso compartido. No todos los antivirus bloquean los archivos descargados a través de programas de uso compartido, así que debe verificar las capacidades de su programa antivirus y los ajustes (settings) que tiene. Además, debe evitar descargar archivos con extensiones del tipo .exe, .scr, .lnk, .bat, .vbs, .dll, .bin, y .cmd.

- Hable con su familia sobre el tema del uso compartido de los archivos. Es posible que los padres no estén al tanto de que sus hijos descargaron programas que operan en red compartiendo los archivos de la computadora familiar y que tal vez puedan haber intercambiado, juegos, videos, música, pornografía u otro material que podría ser inapropiado para ellos. También puede suceder que, como algunas veces los archivos de otras personas pueden estar etiquetados incorrectamente, los niños los descarguen involuntariamente. Además, quizás los niños no estén en condiciones de comprender los riesgos de seguridad y de otro tipo que acarrea el uso compartido de archivos y pueden instalar el programa incorrectamente permitiéndole a cualquier navegante del Internet el acceso a los archivos privados de la computadora familiar.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales y para proveer información de utilidad al consumidor con el objetivo de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite ftc.gov/espanol o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (Consumer Sentinel) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero

Julio 2005

EXHIBIT 9

United States of America
Federal Trade Commission

The Procrustean Problem with Prescriptive Regulation

Remarks of Maureen K. Ohlhausen[1]
Commissioner, U.S. Federal Trade Commission

Sixth Annual Telecom Policy Conference
Free State Foundation
Washington, DC

March 18, 2014

I. Introduction

Thank you to the Free State Foundation for inviting me to speak today. I am honored to participate in today's thoughtful discussion on the future of communications regulation.

At the Federal Trade Commission ("FTC"), protecting consumers and competition on the Internet is a substantial and growing part of our work, and I have some specific ideas on the FTC's future role. After introducing the work of the FTC, I will make three points today. First, to protect consumers effectively while promoting innovation, regulators must embrace regulatory humility and focus on consumer harm. Next, the recent *Verizon* decision is an example of the difficulties of using prescriptive *ex ante* rulemaking to regulate a dynamic industry.[2] The Greek myth of Procrustes and his iron bed is instructive here, as I will explain. Finally, reformers

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

[2] *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. Jan. 14, 2014).

"unfair and deceptive acts."[23] The Act applies across all industries with a few exceptions. And where the FCC's regulations generally set the boundaries of what certain types of entities can do, the FTC's statute fences off deceptive or unfair practices for all entities, but generally permits everything else. The FTC's process is enforcement-centric rather than rulemaking-centric. As such, it is *ex post* rather than *ex ante* and case-by-case rather than one-size-fits-all. And because an enforcement action requires a complaint and a case to move ahead, the FTC's method typically focuses on actual, or at least specifically alleged, harms rather than having to predict future harms more generally.

Because of these structural differences, the FTC's enforcement process is less affected by the systemic knowledge problems of the FCC's prescriptive *ex ante* rulemaking approach. First, rather than having to collect detailed knowledge about an entire industry, the FTC need only gather enough information about the specific parties to the dispute and their behaviors in the relevant market. The FTC has significant investigatory authority to gather such information. Second, collecting such information is much simpler because the vast majority of the necessary information will be in the hands of the parties to the case. Third, even in rapidly changing industries, the FTC's decision on a case will bind only those parties to the specific case. The case will have precedential value, but when the FTC weighs that precedent in future cases, it can then consider any changes in the underlying facts.

Thus, the FTC's approach facilitates what Adam Thierer calls "permissionless innovation," or the "anti-precautionary principle" better than a prescriptive rulemaking approach.[24] The proof, as they say, is in the pudding. As the Internet has become an

---

[23] 15 U.S.C. § 45(a)(1).

[24] *See* Adam Thierer, *Who Really Believes in "Permissionless Innovation"?*, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation/ (last visited Mar. 18, 2014).

increasingly integral part of society, the FTC's enforcement-centric approach has enabled it to serve an increasingly large role in protecting consumers and competition online even while the industry has continued to innovate. In fact, the FTC is already addressing major Internet-centric concerns, including new issues in privacy, fraud, advertising and other consumer protection issues, along with competition issues.

Perhaps the most significant Internet issue the FTC has tackled is privacy. The FTC leads the federal effort to protect the privacy of consumers online. Online privacy is a very wide-ranging topic, covering spam email, data collection and security, safety of children, and online advertising. Hot new topics include the Internet of Things and big data. The FTC has been active in all of these areas, using a full range of tools, including enforcement, consumer and business education, policy research, and convening stakeholders for discussion.

For example, the FTC has brought a wide range of enforcement cases addressing consumer harms related to the Internet, including more than 100 spam and spyware cases and 50 data security cases. The FTC has brought these cases against a wide range of defendants, including an international hotel chain, a major data broker, a national drugstore chain, and the social media site, Twitter. We also hold companies to the promises made in their privacy policies and have brought actions against companies such as Google and Facebook for violating those promises. Additionally, we have brought over 20 cases to enforce the Children's Online Privacy Protection Act and have collected more than $7 million in civil penalties.[25] I believe this strong enforcement record reflects the FTC's readiness and capability to protect consumer privacy online in the face of technological change.

---

[25] *See generally,* Maureen K. Ohlhausen, Commissioner, Fed. Trade Comm'n, *Forum for EU-U.S. Legal- Economic Affairs*, Remarks at The FTC's Privacy Agenda for the 2014 Horizon (September 14, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/ftc%E2%80%99s-privacy-agenda-2014-horizon-forum-eu-u.s.legal-economic-affairs/130914berlinprivacyin2014.pdf.

Enforcement is the cornerstone of our activity to protect consumers online. But it is supported by a wide range of other complementary tools that the FTC uses to promote consumer welfare and competition online, including consumer and business education and policy R&D efforts.

In some respects, the Commission's consumer and business education efforts affect a greater percentage of American consumers than anything else we do. For example, the information available on our webpages to help consumers avoid becoming victims of identity theft and to mitigate the damage of identity theft have had millions of hits and has been distributed widely in hardcopy. We also educate consumers on how to avoid falling victim to online scams, how to deal with spam email, how to protect their computers, phones, and home networks, and how to keep children safe online, among many other topics. For businesses we offer a wide range of legal resources, guidance, and handbooks on topics including online advertising, privacy laws, and best practices across the Internet, including websites, mobile apps, and general data security.

The FTC also has a strong policy research and development capability that it uses to stay abreast of new technologies and emerging issues. For example, the Commission has been closely studying the related issues of big data and the Internet of Things. The FTC has hosted successful workshops on these topics and others, including disclosures of online marketing and advertising practices, children's online privacy and new technology, and mobile device tracking. Future FTC workshops will cover topics such as consumer behavioral prediction and analysis and consumer generated health data. These workshops are particularly valuable because not only do they educate consumers and businesses, they also help the Commission stay informed about the ongoing technological developments and the benefits and risks of such new technologies.

EXHIBIT 10

1 UNITED STATES OF AMERICA
2 BEFORE THE FEDERAL TRADE COMMISSION
3 OFFICE OF THE ADMINISTRATIVE LAW JUDGES
4
5 In the Matter of:)
6 LabMD, INC., a corporation) Docket No.
7 Respondent.) 9357
8 - - - - -
9 DEPOSITION OF DANIEL KAUFMAN
10 Washington, D.C.
11 Monday, April 14, 2014
12 The deposition of DANIEL KAUFMAN was convened
13 on Monday, April 14, 2014, commencing at 10:42
14 a.m., at the offices of the Federal Trade
15 Commission, 600 Pennsylvania Avenue, N.W.,
16 Washington, D.C., before Karen K. Brynteson,
17 Registered Merit Reporter, Certified Realtime
18 Reporter, and Notary Public.
19
20 - - - - -
21
22

1 to allegations of consumer injury. So you can
2 answer to the extent you know.
3 THE WITNESS: Yeah, I do think that
4 the allegations all focus on natural persons, so
5 yes.
6 MR. SHERMAN: Okay. I need to take a
7 break.
8 (A recess was taken at 2:32 p.m., after
9 which the deposition resumed at 2:40 p.m.)
10 MR. SHERMAN: Back on the record. I
11 want to place this on the record, counsel.
12 My next line of inquiry would be to
13 question Mr. Kaufman and the Bureau about the
14 data security standards that they are going to
15 use to basically demonstrate that LabMD
16 participated in an unfair practice.
17 It is my understanding that you have
18 made an objection to that line of inquiry.
19 MS. VAN DRUFF: I believe that the
20 Court had made a determination that that line of
21 inquiry is not permissible.
22 MR. SHERMAN: Okay. I think I just

1 want to place on the record that I disagree with
2 your objection. I believe that what the Court
3 stated was that we could not require -- inquire
4 generally into legal standards, and this is on
5 page 7, second -- the first full paragraph, that
6 we could not -- that we could not inquire
7 generally into the legal standards of the FTC
8 used in the past, and it is currently using to
9 determine whether an entity's data security
10 practices are unfair under Section 5.
11 I do not believe that it prevents us
12 from inquiring about the data security
13 standards. And that is where I want to go next
14 with Mr. Kaufman. And I understand you may have
15 an objection, but I submit that for your
16 consideration.
17 MS. VAN DRUFF: And you are drawing a
18 distinction between the language on page 7 of
19 the Court's March 10th order and the language on
20 page 9 at numbered paragraph 3 of the Court's
21 order; is that correct?
22 MR. SHERMAN: Yes. I am not asking

1 about their decision-making. I want to know
2 what standard LabMD is going to be held to
3 throughout the period.
4 The data security standard, not the
5 legal standard, not reasonableness.
6 MS. VAN DRUFF: Okay. And so to be
7 clear, counsel, if you were to frame your
8 question in terms of the factual bases of the
9 allegations of paragraph 10, which has several
10 subparagraphs, I may be able to permit Mr.
11 Kaufman to answer, but otherwise -- and that is
12 consistent with the Court's holding on page 6 of
13 the March 10th opinion.
14 MR. SHERMAN: The other question,
15 counsel, is given your narrow interpretation of
16 the Judge's order, I know that you have probably
17 prepared your witness based on your
18 interpretation of that order. Is Mr. Kaufman
19 prepared to respond to questions which would ask
20 him what the data security standards are for
21 certain time periods that LabMD will be measured
22 up against?

1 MS. VAN DRUFF: I can't begin to
2 answer that question in the abstract. I would
3 need to know what the question was, and then
4 that may go to a privilege, so I don't know that
5 I can submit to you whether Mr. Kaufman was
6 prepared on a specific subject or not by
7 counsel.
8 MR. SHERMAN: Okay.
9 BY MR. SHERMAN:
10 Q. Mr. Kaufman, paragraph 10 of the
11 Bureau's complaint indicates that at all
12 relevant times LabMD engaged in a number of
13 practices that taken together failed to provide
14 reasonable and appropriate security for personal
15 information on its computer networks.
16 Among other things in paragraph A it
17 says that, it alleges that LabMD did not
18 develop, implement, or maintain a comprehensive
19 information security program to protect
20 consumers' personal information.
21 And I am reading from the complaint.
22 Do you have a copy of the complaint?

1 A. No.
2 Q. We didn't provide you with a copy of
3 the complaint? I had a copy of the complaint
4 for everyone.
5 (Deposition Exhibit Number RX-9 was marked
6 for identification.)
7 MS. VAN DRUFF: I'm sorry, counsel,
8 was there a question pending?
9 MR. SHERMAN: No. I wanted to make
10 sure that the witness had a copy of the
11 complaint in front of him.
12 BY MR. SHERMAN:
13 Q. Based on the allegations in paragraph
14 10(a), my question is has the Bureau or the FTC
15 published, and by published I mean made
16 available to the public, the standard that it
17 requires for a comprehensive information
18 security program for companies like LabMD to
19 have in place?
20 MS. VAN DRUFF: I object to the
21 question because it exceeds the bounds of the
22 Court's March 10th, 2014 protective order, and I

1 am instructing Mr. Kaufman to not answer the
2 question.
3 If you would like to reframe the
4 question as it relates to paragraph 10(a), in
5 terms of the factual bases of Complaint
6 counsel's allegations, I will permit Mr. Kaufman
7 to answer.
8 MR. SHERMAN: Okay.
9 BY MR. SHERMAN:
10 Q. So is there a factual bases for the
11 allegation that LabMD did not develop,
12 implement, or maintain a comprehensive
13 information security program that met the data
14 security standards set out by the Bureau during
15 the year of 2005?
16 MS. VAN DRUFF: And I would make the
17 same objection and the same instruction. Again,
18 at note 6 of the Court's order, the Judge
19 acknowledges that it has already -- that, I'm
20 sorry, the Court has rejected LabMD's argument
21 that it is entitled to discovery of the
22 standards the Commission used in the past and is

1 currently using to determine whether an entity's
2 data security practices violate Section 5.
3 So if you would like to inquire of Mr.
4 Kaufman the factual bases of the allegation of
5 paragraph 10(a), you may ask that question, but
6 as it relates to standards, I will instruct Mr.
7 Kaufman --
8 MR. SHERMAN: I want to know -- I am
9 not going to change my question.
10 BY MR. SHERMAN:
11 Q. I want to know what the data security
12 standards are, okay, and were for the year 2005,
13 that the Bureau published and made known to
14 companies like LabMD with regard to
15 implementing, developing, maintaining a
16 comprehensive information security program to
17 protect consumers' personal information?
18 MS. VAN DRUFF: And I am lodging the
19 same objection. That question exceeds the
20 bounds of the Court's protective order. And I
21 am instructing Mr. Kaufman to not answer the
22 question.

1 BY MR. SHERMAN:
2 Q. And I would ask the same question for
3 the year 2005, 2006, 2007, 2008, 2009, 2010, and
4 through the years to the present for each
5 subcategory in paragraph 10.
6 So, in other words, my question is
7 were the data security standards published and
8 made known to companies like LabMD that the
9 Bureau and/or the FTC made known that establish
10 what a company should do and to what extent it
11 should develop, implement, and maintain a
12 comprehensive information security program to
13 protect consumers' personal information? I
14 would go to subparagraph 10(b), what did the
15 Bureau do and what were the standards that the
16 Bureau published and made known to companies
17 like LabMD requiring them to use readily
18 available measures to identify commonly known or
19 reasonably foreseeable security risks and
20 vulnerabilities on its networks from the year
21 2005 through the present, and I would ask a
22 similar question for each subcategory in

1 paragraph 10.
2 And so is it still your position that
3 you would object to each of those questions and
4 instruct Mr. Kaufman not to answer?
5 MS. VAN DRUFF: Without a pending
6 question, I don't know that I can respond to
7 that, but what I can tell you is the question as
8 it is formulated as I understand it relating to
9 A and B exceeds the bounds of the Court's March
10 10th, 2014 protective order, and I am
11 instructing Mr. Kaufman to not answer that
12 question.
13 MR. SHERMAN: I will go through each
14 question then, okay?
15 MS. VAN DRUFF: Okay.
16 BY MR. SHERMAN:
17 Q. So just to be clear, Mr. Kaufman, I
18 would like to know what are the data security
19 standards that were published in any way, shape,
20 form, or fashion by the Bureau or the FTC that
21 were available and were made known to companies
22 like LabMD about what the FTC's standards or

1 requirements were for the use of readily
2 available measures or what those readily
3 available measures to identify commonly known
4 and reasonably foreseeable security risks and
5 vulnerabilities on its networks were? Can you
6 answer that question?
7 And please keep in mind I am asking
8 for an answer that would encompass the time
9 period of 2005 through the present.
10 MS. VAN DRUFF: And I object to the
11 question on the basis that it is vague,
12 ambiguous, and compound, and that it most
13 importantly exceeds the bounds of the Court's
14 March 10th, 2014 protective order, which limited
15 the topics of this deposition. And I am
16 instructing Mr. Kaufman to not answer the
17 question.
18 BY MR. SHERMAN:
19 Q. Mr. Kaufman, can you tell us what data
20 security standards were published by the Bureau
21 or the FTC to make known to companies like LabMD
22 what the Bureau or the FTC expected in terms of

1 data security standards for that company as it
2 relates to the adequate measures to prevent
3 employees from accessing personal information
4 not needed to perform their jobs?
5 MS. VAN DRUFF: I object to the
6 question because it exceeds the bounds of the
7 Court's March 10th, 2014 protective order
8 insofar as it does not relate to any of the four
9 topics noticed by Respondent and limited by the
10 Court's order, and I am instructing Mr. Kaufman
11 to not answer the question.
12 BY MR. SHERMAN:
13 Q. And, again, I would couch that
14 question for the period of 2005 through the
15 present, and I would note your objection.
16 MS. VAN DRUFF: The same objection,
17 same instruction to not answer the question
18 because it exceeds the bounds of the protective
19 order.
20 BY MR. SHERMAN:
21 Q. Mr. Kaufman, can you tell us what the
22 data security standards are that the FTC

1 published or made known to companies like LabMD
2 which would establish a standard for companies
3 like LabMD to adequately train employees to
4 safeguard personal information from 2005 through
5 the present?
6 MS. VAN DRUFF: Object to the question
7 on the basis that it exceeds the bounds of the
8 Court's March 10th, 2014 protective order. And
9 I am instructing Mr. Kaufman to not answer the
10 question.
11 BY MR. SHERMAN:
12 Q. Mr. Kaufman, what is the standard that
13 the FTC has established, published, and put
14 forth which informs companies like LabMD what
15 the FTC expects with regard to that company's
16 requiring employees or other users with remote
17 access to the networks to use commonly
18 authenticated -- I'm sorry, common
19 authentication-related security measures such as
20 periodically changing passwords, prohibiting the
21 use of the same password across applications and
22 programs, or using two-factor authentication?

1 MS. VAN DRUFF: I object to the
2 question because it exceeds the bounds of the
3 Court's March 10, 2014 protective order. And I
4 am instructing Mr. Kaufman to not answer the
5 question.
6 BY MR. SHERMAN:
7 Q. From the period of 2005 through 2010.
8 I'm sorry, from 2005 to the present. And I note
9 your objection.
10 MS. VAN DRUFF: Same objection,
11 continued instruction. Thank you, counsel.
12 BY MR. SHERMAN:
13 Q. Mr. Kaufman, what are the standards,
14 the data security standards established by the
15 Bureau or the FTC which the Bureau has made
16 known or published and made known to companies
17 like LabMD advising them that the FTC's
18 expectation -- advising them as to what the
19 FTC's expectations were with regard to
20 maintaining and updating operating systems of
21 computers and other devices on its networks, for
22 example, on some computers, Respondent used

1 operating systems that were unsupported by the
2 vendor.
3 Were there any such data security
4 standards and regulations published and made
5 known by the Bureau or the FTC which would
6 advise a company like LabMD what those standards
7 were?
8 MS. VAN DRUFF: Object to the
9 question, which is compound and ambiguous, but
10 also because it exceeds the bounds of the
11 Court's March 10th, 2014 protective order. And
12 I am instructing Mr. Kaufman to not answer the
13 question.
14 BY MR. SHERMAN:
15 Q. And I would include from 2010 through
16 the present.
17 MS. VAN DRUFF: It is the same
18 instruction, same objection.
19 BY MR. SHERMAN:
20 Q. Mr. Kaufman, what are the data
21 security standards established or published,
22 and/or published by the FTC which would inform a

1 company such as LabMD what the FTC's
2 expectations were with regard to that company
3 employing readily available measures to prevent
4 or detect unauthorized access to personal
5 information on its computer networks from 2005
6 through the present?
7 MS. VAN DRUFF: Object to the question
8 because it exceeds the bounds of the Court's
9 March 10th, 2014 protective order. And I am
10 instructing Mr. Kaufman to not answer the
11 question.
12 BY MR. SHERMAN:
13 Q. Mr. Kaufman, has the FTC or the Bureau
14 informed entities like LabMD that the FTC
15 expects or requires them to have a comprehensive
16 information security program?
17 MS. VAN DRUFF: I object to the
18 question because it exceeds the bounds of the
19 Court's protective order. And I am instructing
20 Mr. Kaufman to not answer the question.
21 BY MR. SHERMAN:
22 Q. Mr. Kaufman, has the Bureau or the FTC

1 informed entities like LabMD that the FTC
2 expects and/or requires them to use readily
3 available measures to identify commonly known or
4 reasonably foreseeable security risks and
5 vulnerabilities on its networks?
6 MS. VAN DRUFF: I object to the
7 question because it exceeds the bounds of the
8 Court's March 10th, 2014 protective order, and I
9 am instructing Mr. Kaufman not to answer.
10 BY MR. SHERMAN:
11 Q. Mr. Kaufman, has the FTC informed
12 entities like LabMD that the FTC expects or
13 requires them to use adequate measures to
14 prevent employees from assessing personal
15 information not needed to perform their jobs?
16 MS. VAN DRUFF: I object to the
17 question because it exceeds the bounds of the
18 Court's March 10th, 2014 protective order, and I
19 am instructing Mr. Kaufman to not answer the
20 question.
21 BY MR. SHERMAN:
22 Q. Mr. Kaufman, has the Bureau or the FTC

1 informed entities like LabMD that the FTC
2 expects or requires them to use appropriate
3 measures to prevent employees from installing on
4 their computers applications or materials that
5 were not needed to perform their jobs?
6 MS. VAN DRUFF: I object to the
7 question because it exceeds the bounds of the
8 Court's March 10th, 2014 protective order, and I
9 am instructing Mr. Kaufman to not answer the
10 question.
11 BY MR. SHERMAN:
12 Q. Mr. Kaufman, has the Bureau or the FTC
13 informed entities like LabMD that the FTC
14 expects or requires them to use appropriate
15 measures to adequately maintain or review
16 records of activities on their networks?
17 MS. VAN DRUFF: Object to the question
18 because it exceeds the bounds of the Court's
19 March 10th, 2014 protective order, and I am
20 instructing Mr. Kaufman to not answer the
21 question.
22 BY MR. SHERMAN:

1 Q. Mr. Kaufman, where can a company like
2 LabMD find the Bureau's or the FTC's data
3 security standards which will inform a company
4 like LabMD what the FTC or the Bureau expects
5 with regard to that company's data security?
6 MS. VAN DRUFF: I object to the
7 question because it exceeds the bounds of the
8 Court's March 10th, 2014 protective order, and I
9 am instructing Mr. Kaufman to not answer the
10 question.
11 BY MR. SHERMAN:
12 Q. Mr. Kaufman, with regard to data
13 security standards, does the Bureau or the FTC
14 have the authority to enforce HIPAA?
15 MS. VAN DRUFF: Objection, counsel.
16 Are you grounding any -- are you grounding your
17 question in any of the topics noticed by
18 Respondent or as limited by the Court's March
19 10th, order?
20 MR. SHERMAN: Yes. And it is the
21 objectionable topic of data security standards.
22 MS. VAN DRUFF: I see.

1 MR. SHERMAN: The topic which you have
2 been objecting to.
3 MS. VAN DRUFF: Thank you, counsel.
4 May I have the question read back, please?
5 THE REPORTER: "Question: Mr.
6 Kaufman, where can a company like LabMD find the
7 Bureau's or the FTC's data security standards
8 which will inform a company like LabMD what the
9 FTC or the Bureau expects with regard to that
10 company's data security?"
11 MS. VAN DRUFF: I object to the
12 question because it exceeds the bounds of the
13 Court's March 10th, 2014 protective order, and I
14 am instructing Mr. Kaufman to not answer the
15 question.
16 BY MR. SHERMAN:
17 Q. With regard to data security, does the
18 Bureau or the FTC have the authority to enforce
19 HITECH?
20 MS. VAN DRUFF: I object to the
21 question because it exceeds the bounds of the
22 Court's March 10th, 2014 protective order, and I

1 am instructing Mr. Kaufman to not answer the
2 question.
3 MR. SHERMAN: Can we go off the
4 record?
5 MS. VAN DRUFF: Certainly.
6 MR. SHERMAN: I need to take a break
7 and consult with my counsel.
8 MS. VAN DRUFF: Of course.
9 (A recess was taken at 3:05 p.m., after
10 which the deposition resumed at 3:06 p.m.)
11 BY MR. SHERMAN:
12 Q. Mr. Kaufman, I am going to show you
13 what has been marked as RX-10, which for the
14 record is the expert report of Raquel Hill.
15 (Deposition Exhibit Number RX-10 was marked
16 for identification.)
17 BY MR. SHERMAN:
18 Q. Have you seen that document before?
19 A. Yes.
20 Q. Are the requirements set out in
21 Professor Hill's report what the Bureau will
22 measure LabMD's performance in terms of its data

1 security against at the hearing?
2 MS. VAN DRUFF: I'm sorry, I am going
3 to need the question read back.
4 THE REPORTER: "Question: Are the
5 requirements set out in Professor Hill's report
6 what the Bureau will measure LabMD's performance
7 in terms of its data security against at the
8 hearing?"
9 MS. VAN DRUFF: And, counsel, not
10 trying to be difficult but, of course, the
11 Bureau is not the fact finder at the hearing, so
12 is your question what the Bureau's standard will
13 be at the hearing?
14 BY MR. SHERMAN:
15 Q. Well, my question is you would agree
16 that in Professor Hill's report, there are
17 several descriptions of what Professor Hill
18 opines to be adequate data security measures
19 that should have been taken by LabMD in order to
20 adequately protect the information that it
21 possessed, correct?
22 MS. VAN DRUFF: Objection, Professor

1 Hill's report speaks for itself, but you may
2 answer the question.
3 THE WITNESS: That's my understanding,
4 yes.
5 BY MR. SHERMAN:
6 Q. Okay. And you have read the -- you
7 have reviewed the report, correct?
8 A. Correct.
9 Q. Okay. My question is is that the data
10 security standard that LabMD will be held to in
11 terms of whether or not its data security
12 practices and procedures from 2005 through, I
13 think, July of 2010, is that what -- is that the
14 standard that LabMD will be held to at the
15 hearing?
16 MS. VAN DRUFF: And, counsel,
17 questions relating to standards exceed the
18 bounds of the Court's March 10th, 2014
19 protective order. To the extent you want to
20 rephrase your question as it relates to factual
21 bases for the allegations of paragraph 10, I
22 will permit Mr. Kaufman to answer, but otherwise

1 I am instructing Mr. Kaufman to not answer the
2 pending question.
3 BY MR. SHERMAN:
4 Q. Mr. Kaufman, if it is demonstrated at
5 the hearing that -- well, let me ask you this:
6 The requirement set out in Professor Hill's
7 report with regard to data security, does the
8 Bureau intend to apply these particular
9 standards to other companies?
10 MS. VAN DRUFF: And, again, counsel,
11 to the extent that your question relates to
12 standards or the investigational prosecution of
13 other targets, it exceeds the bounds of the
14 Court's March 10th, 2014 protective order. And
15 I am instructing Mr. Kaufman not to answer the
16 question.
17 BY MR. SHERMAN:
18 Q. Mr. Kaufman, in terms of the data
19 security standards set out in Professor Hill's
20 report, is it the Bureau's position that if
21 LabMD did not take every measure set out in this
22 report, that LabMD has committed an unfair act

1 or practice?
2 MS. VAN DRUFF: Can I have the
3 question read back, please?
4 THE REPORTER: "Question: Mr.
5 Kaufman, in terms of the data security standards
6 set out in Professor Hill's report, is it the
7 Bureau's position that if LabMD did not take
8 every measure set out in this report, that LabMD
9 has committed an unfair act or practice?"
10 MS. VAN DRUFF: The question is
11 predicated on data security standards, and as
12 such it exceeds the bounds of the Court's March
13 10, 2014 protective order, and I am instructing
14 Mr. Kaufman to not answer that question.
15 MR. SHERMAN: Based on that, counsel,
16 I don't have any further questions. What I
17 would like to do is to attempt, at least, to get
18 the ALJ on the phone, not today but some day
19 where we can discuss whether or not your
20 objections will be sustained to that line of
21 questioning.
22 And so that's, that's my intent.

1 MS. VAN DRUFF: Thank you, counsel.
2 MR. SHERMAN: Thank you, Mr. Kaufman.
3 THE WITNESS: Thank you.
4 (Whereupon, at 3:12 p.m., the
5 deposition was concluded.)
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

EXHIBIT 11

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	
	)	
LabMD, Inc.,	)	Docket No. 9357
a corporation,	)	
Respondent.	)	
	)	

COMPLAINT COUNSEL'S ANSWER AND OBJECTIONS TO RESPONDENT'S FIRST SET OF REQUESTS FOR PRODUCTION OF DOCUMENTS (NUMBERS 1-17)

Pursuant to Sections 3.31 and 3.37 of the Federal Trade Commission's Rules of Practice, Complaint Counsel hereby responds to Respondent LabMD, Inc.'s First Set of Requests for the Production of Documents ("Respondent's Requests"). Subject to the General and Specific Objections below, and without waiving these objections, Complaint Counsel answers as follows:

General Objections

The following General Objections apply to each request for documents in Respondent's Requests and are hereby incorporated by reference into each response. The assertion of the same, similar, or additional objections or the provision of partial answers in response to an individual request does not waive any of Complaint Counsel's General Objections as to the other requests.

1. Complaint Counsel objects to Respondent's Requests to the extent they seek to impose duties and obligations upon Complaint Counsel beyond those imposed by the Commission's Rules of Practice for Adjudicative Proceedings, including seeking documents that are beyond the scope of permissible discovery under Rule 3.31(c)(2).

8. All documents sufficient to show what data-security standards are currently used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act.

Complaint Counsel refers Respondent to its response to Document Request 10.

9. All documents sufficient to show what changes occurred in the data-security standards used by FTC to enforce the law under Section 5 of the Federal Trade Commission Act from 2005 to the present and the dates on which these standards changed.

Complaint Counsel objects to this Document Request as vague and ambiguous. Complaint Counsel refers Respondent to its response to Document Request 10.

10. All documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

To the extent this Document Request seeks information in the possession, custody, or control of the Commissioners, the General Counsel, or any Bureau or Office not involved in this matter, Complaint Counsel further objects to this Document Request. Documents in the

possession, custody, or control of the aforementioned entities must be sought through written motion under the procedure laid out in Rule 3.36, 16 C.F.R. § 3.36.

Complaint Counsel further objects to this Document Request to the extent it seeks documents that are protected by the work product doctrine, government deliberative process privilege, government informer privilege, law enforcement investigatory privilege, or common interest privilege.

Complaint Counsel further objects to this Document Request as vague and ambiguous.

Subject to and without waiving any General or Specific objections, Complaint Counsel states that is has previously produced responsive, discoverable, and non-privileged documents at FTC-000685 to FTC-000893and will produce responsive, discoverable, and non-privileged documents.

11. All documents provided to the FTC pursuant to any Civil Investigation Demand regarding its investigation of LabMD.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

Complaint Counsel further objects to this Document Request to the extent it seeks documents that are protected by the work product doctrine, government deliberative process

privilege, government informer privilege, law enforcement investigatory privilege, or common interest privilege.

Complaint Counsel further objects to this Document Request to the extent the requested documents that were provided by Respondent can be obtained directly by Respondent through less burdensome means.

Complaint Counsel further objects to this Document Request to the extent it seeks production of materials previously produced to Respondent.

Subject to and without waiving any General or Specific objections, Complaint Counsel states that it has previously produced responsive, discoverable, and non-privileged documents at FTC-PRI-000001 to FTC-PRI-001724 and refers Respondent to the documents Respondent produced, which have been Bates labeled FTC-LABMD-000001 to FTC-LABMD-003851.

12. All documents identifying LabMD and other companies whose documents or files Tiversa downloaded from Peer to Peer Networks which contained Personal Identifying Information and or Protected Health Information that were provided to FTC.

In addition to the General Objections, Complaint Counsel specifically objects to this Document Request to the extent it seeks to impose duties and obligations upon Complaint Counsel beyond the Commission's Rules of Practice for Adjudicative Proceedings. Complaint Counsel further objects that any such documents unrelated to the FTC's investigation of LabMD and preparations for this hearing are not relevant to the allegations of the Complaint, to the proposed relief, or to the defenses asserted by Respondent. Complaint Counsel further objects to this Document Request as overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence, and an improper inquiry into the mental processes of the Commissioners and FTC attorneys.

EXHIBIT 12

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, INC.,	)	
	)	
Plaintiff,	)	
v.	)	
	)	Civil Action No.: 1:14-CV-810-WSD
FEDERAL TRADE COMMISSION,	)	
	)	
Defendant.	)	

EXPERT OPINION DECLARATION OF CLIFF BAKER

In accordance with 28 U.S.C. § 1746, the declarant, Cliff Baker states:

1. I am Cliff Baker. I submit this declaration for use in the lawsuit *LabMD v. Federal Trade Commission.* I offer this declaration to respond to statements in the Expert Report of Professor Hill and how her opinions on data security relate to requirements on data security for HIPAA-covered medical service providers imposed by the Department of Health and Human Services. HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. I base my declaration on my personal knowledge and professional experiences.

2. I, Cliff Baker, have had the following roles in my career in the field of data security:

a. Director in the Healthcare Information Security practice at PricewaterhouseCoopers. I led the security practice nationally for the Healthcare Consulting practice. I worked at PricewatershouseCoopers for 14 years and consulted with clients nationally on implementing security programs and practices. An example of a project I led was a establishing a program that included four state healthcare associations. The program included meeting, discussing and educating over 50 organizations on adopting security measures to comply with HIPAA.

b. Chief Strategy Officer for HITRUST. I joined HITRUST in 2008 to lead the creation of the Common Security Framework, which is a healthcare industry framework based on globally recognized standards, such as ISO 27001/2 and NIST. A key objective of the framework is to provide a prescriptive and scalable reference for covered entities to determine reasonable and appropriate controls to implement for their organizations. The controls are tailored to the size and operations of the organization. I facilitated working sessions with over 200 security professionals from the healthcare

industry, security technology companies, consulting companies, and government entities in the development of the framework.

c. Founder and Managing Partner of Meditology Services. Meditology Services was founded in 2010 to provide privacy and security services to healthcare clients. I employ former Chief Information Security and Privacy Officers that were responsible for implementing security at their healthcare organizations. We provide consulting services in the areas of compliance with HIPAA and the implementation of privacy and security programs for healthcare organizations ranging from small providers to global healthcare organizations.

3. I have spent over 19 years working in the healthcare and information security fields. This experience has provided me with first-hand knowledge about the challenges and practical realities faced by healthcare organizations in securing Protected Health Information (PHI).

4. The 1996 HIPAA Statute states that in promulgating information security regulations, the Secretary must take into account "the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary)," and the preamble to the HIPAA Security

Rule (p. 8335) states accordingly that one of the foundations of the rule is that "it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes."

5. The process by which HHS promulgated the initial final HIPAA Security Rule involved reviewing and responding to approximately 2,350 timely public comments, balancing the interests of health care professionals and firms with patient-related interests. Based on these public comments, HHS crafted a unique information security regulatory scheme that separated "implementation specifications" – the types of very specific security requirements emphasized by the FTC's expert – into two classes: "required" and "addressable". HHS stayed consistent with this structure in its most recent updates to the HIPAA Privacy and Security rules in 2013. This structure reflects HHS' challenge in complying with Congressional intent in establishing a security rule to address reasonable and appropriate security requirements for the range of organizations in healthcare that differ greatly in operations, size, complexity, and resources. For example, a single physician practice may differ significantly from the way in which it addresses security as compared to a multi-national health plan. The physician practice will probably not employ dedicated technology or security personnel and will rely heavily on guidance from HHS. The practice will also rely predominantly on

security that is provided by default settings and software vendor recommendations and will implement mostly manual procedures to manage and monitor access to patient information and associated Information Technology (IT) systems. On the other end of the spectrum, a national health system will likely hire a team of experienced security professionals that may even exceed the total number of employees in these small practices. These larger organizations will buy and build the most advanced and sophisticated solutions available in their efforts to protect sensitive patient data.

6. HIPAA demands that a covered entity perform a risk assessment in good faith and take actions to secure Electronic Protected Health Information (EPHI) based on the findings of that risk assessment. HIPAA's security requirements are also explicitly "scalable" based on the size of the entity. Therefore, to assess HIPAA noncompliance, it is necessary to determine if a risk assessment was performed in good faith, and resulted in a process that included implementation of requirements and appropriate responses to "addressable" issues. These responses are all subject to different standards and scalable so that they could be implemented effectively by covered entities of all types and sizes. Given the limited knowledge of information technology by many small health care providers, especially during the early years of HIPAA Security,

many of the security measures they were advised to adopt by HHS issued guidance related to physical and administrative security rather than specific technical security.

7. The preamble to the Rule makes the balancing of interests and the assessment of feasibility for small providers by HHS, employing notice and comment rulemaking, quite transparent at many points. For example, in connection with encryption of data in transit, which corresponds to Section 164.312(e)(1) of the Rule on Transmission Security, the preamble notes (FR V. 68, #34 at 8357):

> [W]e agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification.

8. This concept was reinforced by CMS in a seven-part series published to provide guidance to the industry for complying with HIPAA. In Volume 2 Security Standards: Implementation for Small Provider of the HIPAA Security Series published in December 2007, CMS states:

> All covered entities must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to EPHI (see 45 C.F.R § 164.302.). Small providers that are covered entities have unique business and technical environments that provide both opportunities and challenges related to compliance with the Security Rule. As such, this paper provides general guidance to providers such as physicians and dentists in solo or small group practices, small clinics, independent pharmacies, and others who may be less likely to have IT staff and whose approach to compliance would generally be very different from that of a large health care system. It is important to note however, that this paper does not define a small provider, nor does it prescribe specific actions that small providers must take to become compliant with the Security Rule.

9. These comments reflect the challenges of small providers in the early years of HIPAA, but even as more recently as 2013 and 2014, HHS is still publishing security guidance for small providers, and the guidance is still elementary in nature. This is reflected by the following list of recommendations published in the most recent version of the Guide to Privacy and Security of Health Information, published by the Office of the National Coordinator for Health Information Technology in 2013:

> Remember the Basics
>
> - Is your server in a room only accessible by authorized staff? Do you keep the door locked?
> - Are your passwords easily found (e.g., taped to a monitor)? Easy to guess?

- Do you have a fire extinguisher that works?
- Where, when, and how often do you back-up? Is at least one back-up kept offsite? Can your data be recovered from the back-ups?
- How often is your EHR server checked for viruses?
- Who has keys to your building? Any former employees or contractors?
- What is your plan for what to do if your server crashes and you cannot directly recover data? Do you have documentation about what kind of server it was, what software it used, etc.?

10. These recommendations reflect HHS' understanding of the realities associated with implementing security for small providers in the healthcare industry. After almost ten years of complying with HIPAA security rules, the guidance has not changed substantively for small practices. In more recent years, HHS has focused on requiring security functionality to be built into applications for the healthcare industry, so providers will have many security controls by default and not have to rely on expertise, additional tools and resource intensive processes to protect information.

11. I have reviewed Dr. Hill's Report, and believe that the standards articulated by Dr. Hill are:

a. Confusing by introducing additional security principles (i.e., 7 security principles referenced by Dr. Hill) that are difficult to reconcile with the Administrative, Technical and Physical main structure of the HIPAA security rule.

b. Not scalable in accordance with the Security Rule, and not taking account as required by the 1996 HIPAA Statute of "the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary). For example, the recommendation for file integrity monitoring requires expertise to implement and configure these solutions and can be even more resource intensive to understand, investigate and resolve alerts produced by the solution. In my experience, I very rarely observe adoption of this technology by small providers in the industry.

c. More prescriptive than HIPAA or inconsistent with HHS guidance, including encryption at rest (an addressable requirement of 164.312(a)(1)), encryption in transit (an addressable requirement

of 164.312(e)(1)), intrusion detection (not addressed specifically by the Security Rule), virus protection (an addressable requirement of 164.308(a)(5) (ii)(B)), firewalls (not addressed specifically by the Security Rule), penetration testing (not addressed by the Security Rule), and file integrity monitoring (not addressed specifically by the Security Rule). While many of these standards are good security practices, controls such as broad scale encryption at rest are generally not adopted across the industry. The electronic health record certification requirements published for HHS for Meaningful Use Stage 2 in 2012 do not even require this level of encryption for all PHI stored by the system. In addition, tools such as intrusion detection and file integrity monitoring systems require experienced and committed technical resources to configure and manage. Dr. Hill's standards presume a level of knowledge of technical information security generally not available to small health care providers.

d. Contradictory to the guidance provided by HHS. For example, Dr. Hill almost exclusively focuses on technologies or technical processes for the risk assessment process (i.e., antivirus

applications, firewalls, various types of vulnerability scans, intrusion detection systems, penetration tests, file integrity monitoring, and other measures). This is inconsistent with HHS guidance that the risk assessment can be a qualitative and manual process as outlined in the standard referenced by Dr. Hill: Special Publication NIST 800-30 Guide for Conducting Risk Assessments.

12. If health care providers are going to be held to a compliance standard that is simply an expert's opinion of best practices in information security at any point in time, when that expert standard exceeds the published compliance standard developed under HIPAA and the historical guidance provided by HHS, then the standard developed under HIPAA is made effectively meaningless. This will create confusion for Health care providers that will not know what is required of them.

13. I have not reviewed whether LabMD is or was compliant with the HIPAA Security Rule; I suggest only that for HIPAA not to be contradicted and Congressional intent and constitutional process not to be undermined, the information security of HIPAA-covered health care providers must be regulated by an agency with jurisdiction under the properly promulgated HIPAA Security Rule,

which during the time period in question was only the Department of Health and Human Services.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11 day of April, 2014.

CLIFF BAKER

CERTIFICATE OF SERVICE

This is to certify that, on April 11, 2014, I electronically filed the foregoing **EXPERT OPINION DECLARATION OF CLIFF BAKER** with the Clerk of Court using the CM/ECF system, and served the following by e-mail and U.S. Mail as follows:

LAUREN E. FASCETT, Esq.
Trial Attorney
U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Lauren.Fascett@usdoj.gov

This 11th day of April, 2014.

/s/ Burleigh L. Singleton
Counsel for Plaintiff

EXHIBIT 28

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	
	)	Docket No. 9357
LabMD, Inc.,	)	
a corporation.	)	PUBLIC

ORDER CORRECTING ORAL ARGUMENT TRANSCRIPT

On May 4, 2016, Complaint Counsel filed an unopposed Motion to correct the transcript of the Oral Argument held in this proceeding on March 8, 2016. The Motion states that Complaint Counsel conferred with counsel for Respondent in a good faith effort to stipulate to the desired corrections, as prescribed by Commission Rule 3.52(i), 16 C.F.R. § 3.52(i), and that while Respondent has declined to join the Motion, Respondent agrees to the proposed corrections and will not oppose the Motion. Accordingly,

IT IS ORDERED THAT the Oral Argument Transcript be, and it hereby is, modified to adopt the two corrections requested by Complaint Counsel in the May 4 Motion, and to read as shown in the attached corrected copy.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: May 16, 2016

1 UNITED STATES OF AMERICA
2 BEFORE THE FEDERAL TRADE COMMISSION
3
4 COMMISSIONERS: Edith Ramirez, Chairwoman
5 Maureen K. Ohlhausen
6 Terrell McSweeny
7
8 In the Matter of)
9) Docket No. 9357
10 LabMD, Inc.,)
11 a corporation.)
12
13 March 8, 2016
14 1:00 p.m.
15 ORAL ARGUMENT
16
17 Federal Trade Commission
18 600 Pennsylvania Avenue, N.W.
19 Washington, D.C.
20
21
22
23
24 Reported by: Josett F. Whalen, Court Reporter
25

1 CHAIRWOMAN RAMIREZ: And you don't think it
2 would be reasonable for a company to have some form of
3 monitoring to ensure that those policies were followed?
4 MR. LECHNER: Well, there was testimony that
5 there was monitoring there, but that's the question,
6 why -- and there was no opinion as to what was wrong
7 with that monitoring compared to what the baseline was
8 from time to time to time.
9 There's just a broad brush. There's no attempt
10 to segregate this and look at it from period to period,
11 nor to look at it from whether paragraph 10(a) or right
12 through paragraph 10(g) and break it out seriatim as
13 each of those moved on from year to year to year.
14 COMMISSIONER McSWEENY: Let me just back up
15 because I am confused about this argument that there were
16 no standards in place during this period of time that
17 you could follow.
18 MR. LECHNER: I'm sorry?
19 COMMISSIONER McSWEENY: Aren’t we talking
20 about HIPAA-covered documents, medical records, and
21 hopefully state standards here as well?
22 MR. LECHNER: Well, that's just the point.
23 Professor Hill said she was not familiar with HIPAA.
24 Professor Hill did not link any standard to this industry
25 in particular or to this business in particular, and the

1 reasonableness demands both.
2 You cannot use a broad brush with regard to the
3 industry in general. What industry would it be? The
4 security industry? Would it be the computer industry?
5 Or is it the industry of the accumulation of medical
6 data for legitimate purposes, as LabMD was involved in?
7 But that's another point that was not done
8 here. There are no base standards with regard to the
9 particular company involved. And as the Commission
10 pointed out, that's what has to be done in order to look
11 at what reasonableness is. It's based upon the
12 circumstances.
13 What are the circumstances? The company in
14 question, the size of it, what it does, how it does it,
15 what its business involved, and over what period of time
16 are we looking at it and how did those standards
17 change.
18 There was no testimony at even the basic
19 that the standards remained the same the whole time.
20 And I think it was acknowledged, again to go
21 back to your order on the motion to dismiss, that this
22 technology is rapidly changing, if not day to day, at
23 least much more quickly than one would expect.
24 CHAIRWOMAN RAMIREZ: Well, what I think the
25 Commission stated in its decision was that it's a

1 COMMISSIONER McSWEENY: Can I focus on a period of
2 time here for just a second, because I am a little
3 confused about what period of time we're talking about.
4 In your brief, you focus, I think, on the 2007 to
5 2008 time frame. Dr. Hill's testimony focuses on
6 2005 to 2010. Complaint counsel has mentioned that you
7 still have a lot of sensitive information and some
8 ongoing issues, in their view, surrounding how that
9 information is being protected.
10 What steps is LabMD taking at this point
11 to ensure that highly sensitive information
12 is being protected? And in your view, what is the
13 relevant period of time that we should be considering?
14 MR. LECHNER: Well, it's my understanding that
15 LabMD is out of business now.
16 COMMISSIONER McSWEENY: But it still has a huge
17 amount of patient information.
18 MR. LECHNER: I don't know how much it has left,
19 but it's not doing business right now as a result of the
20 expense and the problems with this case.
21 That's one of the problems. You know, when the
22 Commission brings something like this, a lot of these
23 cases end up --
24 COMMISSIONER McSWEENY: Let's back up for just
25 a second.

MR. LECHNER: I'm sorry?

COMMISSIONER McSWEENY: What is the relevant period of time?

MR. LECHNER: The relevant period -- I'm sorry. The relevant period of time I'd suggest to this body is May of 2007 to -- June of 2007 to May of 2008.

I know that there's testimony offered to through 2010, but there is absolutely nothing beyond 2010 other than rank speculation and argument. At worst for us it's to 2010.

But more precisely, it's to 2008 because the Sacramento documents are a red herring in this case. And the only thing that we're talking about here is the 1718 File, which there is no testimony that it was viewed by anybody other than Tiversa, Tiversa's professor I think in Dartmouth, the FTC and the people to whom the FTC gave it. That's the only testimony in this case.

COMMISSIONER OHLHAUSEN: But doesn't that go back to the idea that you have to show actual harm versus likely harm?

MR. LECHNER: Yes. Well, that's the point. You can either show actual harm, and if you can't show that, we'll concede that the alternative, the "or" in the disjunctive there, you know, that the alleged

EXHIBIT 29

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**

FINAL ORDER

The Commission has heard this matter upon the appeal of Complaint Counsel from the Initial Decision of the Administrative Law Judge, and upon briefs and oral argument in support thereof and in opposition thereto. For the reasons stated in the accompanying opinion of the Commission, the Commission has concluded that LabMD's data security practices were unreasonable and constitute an unfair act or practice that violates Section 5 of the Federal Trade Commission Act. The Commission has therefore determined to vacate the Initial Decision and issue the following order:

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

2. Unless otherwise specified, "respondent" shall mean LabMD, Inc., and its successors and assigns.

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before July 28, 2016, including, but not limited to, consumers listed in the Insurance File and other documents available to a peer-to-peer file sharing network, but excluding consumers whom LabMD has notified, before July 28, 2016, of a data security breach.

4. "Insurance File" shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network.

5. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

I.

IT IS ORDERED that the respondent shall, no later than the date this order becomes final and effective, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after July 28, 2016, for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after July 28, 2016, for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part I of this order; and

D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected, and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not

the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, Assessments may be sent by first-class mail, but only if an electronic version of any such Assessment is contemporaneously sent to the Commission at Debrief@ftc.gov.

III.

IT IS FURTHER ORDERED that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of the date this order becomes final and effective unless an appropriate notice has already been provided, as follows:

A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.), and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website (www.ftc.gov/idtheft), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from www.annualcreditreport.com and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and

3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.

B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.

C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after the date this order becomes final and effective, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date this order becomes final and effective, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

This order will terminate on July 28, 2036, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: July 28, 2016

EXHIBIT 30

PUBLIC

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
08 11 2015
SECRETARY

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
BEFORE THE OFFICE OF ADMINISTRATIVE LAW JUDGES

ORIGINAL

In the Matter of	)	**PUBLIC**
LabMD, Inc. a corporation, Respondent.	)	Docket No. 9357

RESPONDENT LABMD, INC.'S
CORRECTED[1] PROPOSED FINDINGS OF FACT

Daniel Z. Epstein
Prashant K. Khetan
Patrick Massari
Cause of Action, Inc.
1919 Pennsylvania Avenue, NW
Suite 650
Washington, DC 20006

Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

Counsel for Respondent

Dated: August 11, 2015

[1] This document was timely filed on August 10, 2015. It is being re-filed solely to correct errors in the redaction process, mostly due to making redactions using a computer tool that does not transmit when converted to pdf and filed electronically. Counsel for LabMD has been in constant discussion with Complaint Counsel as well as Crystal McCoy Hunter in the Office of the Secretary regarding these issues.

PUBLIC

TABLE OF CONTENTS

A. BACKGROUND 4
B. LABMD 7
C. THE ORIGINS OF FTC'S INVESTIGATION OF LABMD 11
D. LABMD'S DATA SECURITY. 31
E. FISK TESTIMONY 66
F. THE "DAY SHEETS." 68
G. LABMD IS REGULATED UNDER HIPAA/HITECH. 69
H. COMMISSION LACKS STANDARDS FOR MEDICAL COMPANIES. 70
I. DR. HILL. 73
J. RICK KAM. 89
K. JIM VAN DYKE. 97
L. PROFESSOR SHIELDS. 107
M. COMPLAINT COUNSEL'S PROOFS. 108
N. THE DAMAGE DONE TO LABMD 115
O. ATTACHMENT 1: RESPONDENT COUNSEL'S EXHIBIT INDEX 1-20
P. ATTACHMENT 2: RESPONDENT COUNSEL'S WITNESS INDEX 21-22

PUBLIC

RECORD REFERENCES

References to the record are made using the following citation forms and abbreviations:

JX# – Joint Exhibit

CX# – Complaint Counsel Exhibit

RX# – Respondent Exhibit

RXD# – Respondent Demonstrative Exhibit

(Name of Witness, Tr. xx – Trial Testimony

JX/CX/RX# (Name of Witness, Dep. at xx) – Deposition Testimony

JX/CX/RX# (Name of Witness, IHT at xx) – Investigational Hearing Testimony

Complaint ¶ x – Complaint Counsel's Complaint filed August 28, 2013

Answer ¶ x – Respondent LabMD, Inc.'s Answer to Complaint

{ bold } – *In Camera* Material

PUBLIC

A. Background

1. The Federal Trade Commission ("FTC" or the "Commission") initiated an investigation of Respondent, LabMD, Inc. ("LabMD") in January 2010.

2. The Commission acted against LabMD based on information obtained from Tiversa, Inc. ("Tiversa"), through the "Privacy Institute" in 2009. (CX0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX0703 (Boback, Dep. at 141-142)).

3. The Privacy Institute was created to share information between the Commission and Tiversa. (CX 0703 (Boback, Dep. at 141-142); (RX 541 (Boback, Dep. at 37-38, 47-49)) (" … [on the] spreadsheet that the Privacy Institute received from Tiversa, which the Privacy Institute later provided to the FTC pursuant to [the] CID, ... [t]here were a list of [approximately 100] companies, names. There were, to the best of my recollection, a listing of how many social security numbers were exposed in a descending order. . . [and] Tiversa created the spreadsheet . . . [because] Tiversa provides security services on file sharing networks in which it is quite common to see large disclosures of social security numbers on these networks. And pursuant to the CID that [information request] went to the Privacy Institute, [and then] Tiversa searched Tiversa's data store for anything responsive of that CID, created the spreadsheet, [and] provided the spreadsheet to the Privacy Institute. And then, the Privacy Institute, pursuant to the CID, provided it to the FTC, to the best of my knowledge."), 54-55 ("I think we already were clear that the Privacy Institute did not have operations … The Privacy Institute didn't do anything.").

4. The Commission and Tiversa collaborated beginning in 2007. (Wallace, Tr. 1346-1349) (Q. "After the testimony at the congressional hearing for which you provided some documentation, did there begin to be communications between Tiversa and the FTC?" A. "Yes."

PUBLIC

Q. "How soon after the congressional hearing did these communications begin?" A. "I couldn't say for sure, but I would venture to speculate maybe around two months after." Q. "And were you present during these communications?" A. "Yes." Q. "And how often were these communications occurring once they began?" A. "There were different things happening, so sometimes there would be communication that was quite frequent, other times, you know, maybe weekly."); (RX644[2] (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? 56 (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA), *available at* http://www.scribd.com/doc/265820770/2015-01-02-Staff-Report-for-Rep-Issa-Re-Tiversa#scribd (last visited Aug. 9, 2015) ("***In October 2007, Boback participated in a conference call with FTC officials"*** **and in "*December 2007, Boback provided documents to the FTC*.**" (emphasis added and citations omitted).

5. As a result of the Commission's collaboration with Tiversa, the Commission issued a February 22, 2010 press release titled "Widespread Data Breaches Uncovered by FTC Probe." (Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Fed. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015).

6. In this press release, the Commission stated: "we found health-related information,

---

[2] Respondent notes this Court's ruling on RX 644: "RX 644 is hereby admitted subject to the following limitations and qualifications as to its evidentiary use: (1) official notice is taken of the fact that the OGR investigated the activities of non-party witness Tiversa, Inc. ("Tiversa") and of the conclusions of the OGR staff as to the truthfulness and completeness of the information provided to the FTC by Tiversa and its president, Robert Boback; (2) statements purportedly made by Mr. Boback to the OGR, to the extent referred to in RX 644, will not be considered for the truth of the matters asserted therein; and (3) documents provided to OGR, to the extent referred to in RX 644 and not previously admitted into evidence in this case, will not be considered for the truth of the matters asserted therein." Order on Respondent's Motion to Admit Exhibits at 3 (July 15, 2015).

PUBLIC

financial records, and drivers' license and social security numbers--the kind of information that could lead to identity theft …" and that it "notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, ha[d] been shared from the organizations' computer networks." (Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015).

7. The information "found" by the Commission was actually given to it by Tiversa. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX 0703 (Boback, Dep. at 141-142)).

8. This information included an insurance aging file (the "1718 File") from LabMD containing personal health information ("PHI"). (Wallace, Tr. 141); (Shields, Tr. 876-881).

9. At all times relevant, the Commission knew or should have known that 42 U.S.C. § 1320d-6 provides that: "[a] person who knowingly and in violation of this part … (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization."

10. At all times relevant, the Commission knew or should have known that Tiversa was not authorized by LabMD or by any of the patients listed on the 1718 File to obtain or disclose the identifiable health information contained therein.. (CX 0679 (Verified Complaint for Declaratory

PUBLIC

and Injunctive Relief (N.D. Ga.), at at 5-6 ¶ 16)) ("At all times relevant, LabMD's Protected Health Information ('PHI'), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), 42 U.S.C. §§ 300jj *et seq*., 17901 *et seq*.").

10. January 2005 through July 2010 is the relevant time period during which the Commission claims LabMD's data security was inadequate, unreasonable and unlawful ("Relevant Time"), (Hill, Tr. 221-222), and that these inadequacies "caused" or are "likely to cause" substantial consumer injury which cannot reasonably be avoided. (Complaint, at 5 ¶ 22 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

11. The Commission has never alleged that LabMD's post-July 2010 data security was inadequate. (Complaint, at 4-5 ¶¶ 17-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357); (CX 0740 (Hill, Rep. at 3-4 ¶¶ 4, 48)) ("This conclusion covers the time period from January 2005 through July 2010 (Relevant Time Period); as I explain in Paragraph 48, below, from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.") ("As I noted in Paragraph 4, above, my overall conclusion and the specific opinions that support that conclusion cover the Relevant Time Period, which is January 2005 through July 2010. From my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.").

B. <u>LabMD</u>

12. LabMD is a small, medical services company providing uro-pathology cancer

PUBLIC

detection services to physician customers. (Daugherty, Tr. 952).

13. LabMD, was incorporated in 1996 by Michael J. Daugherty ("Daugherty"), its President and CEO. (Daugherty, Tr. 939).

14. LabMD began in 1996 primarily as a men's health clinic. (Daugherty, Tr. 939-940).

15. Prior to founding LabMD, Mr. Daugherty worked for 13 years in the hospital and healthcare field as part of Mentor Corporation as a Surgical Sales Technical Representative working in the Urology and Plastic Surgery marketplace. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld, at 2)).

16. While working as a Surgical Sales Representative, Mr. Daugherty was "trained at US Surgical in Connecticut over a two–month period on aseptic technique, patient privacy, confidentiality, surgical technique" and "scrubbed in" with the surgeons. (Daugherty, Tr. 938).

17. LabMD changed its business model in the 1990s to meet a demand in the market for physicians who wanted their tissue samples analyzed by a specialist, which was made possible by mobile ultrasound machines. (Daugherty, Tr. 941-943).

18. Managed care exploded in the 1990s resulting in the requirement that physicians' offices direct tissue samples to a particular laboratory covered by their patients' health insurance. (Daugherty, Tr. 944-945).

19. LabMD's niche in the area of uro–pathology was creating technology whereby physicians' patient databases were coded, so tissue sample requests could be sent to LabMD without physicians' staff needing to spend time coding the samples by hand. (Daugherty, Tr. 959-960) (Q. "So what process did you put in place?" A. ". . . what we did was we would go into a[n] account, a physician's office. We would get their entire insurance database, and we would

PUBLIC

give it a primary additional code. . . . [W]e had the database populated with all the patients that were in the physician's office, so that saved all this time. . . . This is proactivity to increase patient result speed because people want to know if they do or don't have cancer as soon as possible, reduce any pitfalls of error. It's just a win-win everywhere.").

20. The system was set up to limit access of physicians to their patients' information only. (CX 0719 (Hyer, Dep. at 142)).

21. LabMD created a process to streamline the interaction between physicians' offices requesting lab work and LabMD's delivery of the diagnosis of the lab work requested. (Daugherty, Tr. 955-964).

22. LabMD's process resulted in faster lab results turnaround time and fewer diagnosis code errors. (Daugherty, Tr. 961-962).

23. LabMD provided a valuable and necessary service in the uro-pathology marketspace. (Daugherty, Tr. 962) (A. "And in our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices. . . . [T]he amount of errors just fell through the floor. . . . [W]e even knew ahead of time what was coming so that we could be prepared.").

24. The tissue slides were received into the LabMD facility where the histologist puts each sample into its proper cartridge. (Daugherty, Tr. 968; RXD 04).

25. LabMD only analyzed one type of tissue, which allowed for 30-minute processing time as opposed to 12 hours. (Daugherty, Tr. 968-969).

26. After the tissue was completely dehydrated, it was placed in an embedding center

PUBLIC

where hot wax is poured over the sample to hold it firmly in place for cutting. (Daugherty, Tr. 969; RXD 06).

27. The histotech then utilized the microtome "to cut the tissue one cell thick" for testing and analysis. (Daugherty, Tr. 969; RXD 07).

28. The tissue was then placed "in a wax ribbon that is now one cell thick along the ribbon, and … put in a water bath to rehydrate …" (Daugherty, Tr. 970; RXD 08).

29. RXD 10 is a tissue slide with identifying numbers showing case number and exact location within the gland. (Daugherty, Tr. 970-971; RXD 10) (". . . the last two digits are going to show the exact location within the gland. The top number in the center is the case number that is assigned electronically by the software back in the urologist's office when the nurse places the order. So at this point all these slides have had the proper, very legible information put on each one, so the correct tissue ribbon is put on each slide and they're ready to go to be stained.").

30. The tissue sample was then placed in the Sakura stainer, which is part of the diagnosis protocol proper. (Daugherty, Tr. 971; RDX 11) (A. ". . . Different types of cancer cells need different types of stains. And not only is the type of stain relevant, but the amount of time immersed in the stain and the time immersed and the order of immersion is relevant to making the cancer cells pop out so it's easy to diagnose for the physician. . . . this is a phenomenal machine because it is -- it makes sure that every single tissue slide location is stained properly, recorded. It's—it's fantastic.").

31. The tissue slides were then taken out of the stainer and "started to be prepped for the physician's diagnosis to start." (Daugherty, Tr. 972; RXD 12).

32. The tissue sample was then placed into a final folder so the on-site physician at

PUBLIC

LabMD could begin "reading each slide location" and making a diagnosis. (Daugherty, Tr. 973; RXD 13; RXD 14).

33. LabMD retained these samples and made them available to physicians for years. (Daugherty, Tr. 972).

34. LabMD's coding and numbering system benefitted both the patients and physicians it served. (Daugherty, Tr. at 972) (A. ". . . the center number is the accession number. The LM is the location of the gland. The number below L2 is the level, because we'll keep several levels of the tissue because we need to keep this for years to come in case a second opinion is wanted, there's litigation, there's clinical questions years down the road, so we take several levels of the tissue and hold them.").

C. <u>The Origins of FTC's Investigation of LabMD</u>

35. On July 24, 2007, the CEO of Tiversa, Robert Boback ("Boback") testified before a congressional committee concerning the serious data security risks posed by P2P file sharing programs. (Wallace, Tr. 1341-1342).

36. According to CEO Robert Boback, Tiversa was incorporated in 2004. (CX 0703 (Boback, Dep. at 11)).

37. Tiversa provides information and security services which essentially consist of P2P breach detection and remediation. (CX 0703 (Boback Dep. at 10-12); RX 541 (Boback Dep. at 19-21)).

38. Tiversa has nearly 120 patents or patents pending for software providing unique searches of internet file sharing networks. (CX 0703 (Boback Dep. at 10-12); RX 541 (Boback Dep. at 19-21)).

PUBLIC

39. Tiversa has received direct payment from the federal government for providing services to the FBI and the Department of Transportation. (CX 541 (Boback, Dep. at 64, 38-41); (Complaint Counsel's Opposition to Respondent's Motion for Sanctions at 6 n.6 (Aug. 25, 2014)) ("Tiversa received no government funds for the work it performed with researchers at Dartmouth College, including work related to the Data Hemorrhages article, in which the 1718 File is excerpted (CX0382). *See, e.g.*, CX0703 at 134; RX541 at 56.").

40. However, ***in response to an unanticipated question during Complaint Counsel's May 20, 2014 opening statement, Complaint Counsel mistakenly stated that Tiversa had received no federal funding.*** (*Compare* Compl. Counsel's Opposition to Respondent's Motion for Sanctions at 6 (Aug. 25, 2014) *with* RX 541 (Boback, Dep. at 14)).

41. During the November 21, 2013 deposition of Tiversa's Rule 3.33 designee, Complaint Counsel did not develop any facts regarding Tiversa's contracts with government agencies. (CX 0703 (Boback, Dep. at 1-168)).

42. At a Congressional hearing before the House Oversight and Government Reform Committee on July 24, 2007, the Commission testified that it viewed P2P file sharing as a "neutral technology." (CX703 (Boback, Dep. at 139-140); (*Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform,* 110th Cong., 1st Sess. 1 10, 40-84 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last visited Aug. 9, 2015)).

43. The Commission's position at the July 24, 2007 Congressional hearing was:

- "P2P file-sharing ... is a 'neutral' technology" and there was "little empirical evidence" regarding relative P2P risks "compared to the risks from other Internet-related activities."

PUBLIC

- "FTC will continue to assess [P2P] risks..., educate consumers, monitor and encourage [P2P] industry self-regulation, and investigate and institute law enforcement actions [against P2P companies] when appropriate."
- FTC's "twenty-first century law enforcement tools" included "Consumer Sentinel, a secure, online fraud and identity theft complaint database" containing "over 3.9 million fraud and identity theft complaints [that is] accessible to more than 1,650 law enforcement agencies, which use the database to share information, coordinate investigations, and pursue case leads," as well as "Internet Lab, which provides FTC lawyers and investigators with high-tech tools to ... capture web sites that come and go quickly ...[and] FTC staff with the necessary equipment to preserve evidence for presentation in court."

(Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 3, 8 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)) (Statement of Mary Engle, Assoc. Dir. for Advertising Practices. Fed. Trade Comm'n), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf (last accessed Aug. 9, 2015).

44. FTC had not warned businesses of the risk of inadvertent file sharing through LimeWire in February, 2008, when Tiversa hacked LabMD for Tiversa's commercial interest. (Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 10, 40-84 (July 24, 2007), *available at*

PUBLIC

http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)) ("The [2005 FTC Report] emphasized that many of the risks posed by P2P file sharing also exist when consumers engage in other Internet-related activities, such as surfing Web sites, using search engines, or e-mail…."); (FTC Staff Report, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, at 20 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015)) ("***Although it has required warnings with respect to inherently dangerous products, the Commission concluded that it was not aware of any basis under the FTC Act for requiring warnings for P2P file sharing and other neutral consumer technologies***.") (emphasis added).

45. The FTC's considered position for the period of 2005–2008 was that using P2P networks like LimeWire or FrostWire was not in and of itself an unreasonable practice from the viewpoint of data privacy and security. (Prepared Statement of Mary Engle, Fed. Trade Comm'n, Assoc. Dir. for Advertising Practices, Before the U.S. House of Rep. Committee on Oversight and Government, Washington, D.C., at 1–12 (July 24, 2007), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf (last accessed Aug. 9, 2015)).

46. FTC worked with LimeWire and other P2P software providers to encourage industry self-regulation. (Fed. Trade Comm'n, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, Staff Report, at 26 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015))

PUBLIC

("FTC staff encourages the P2P file-sharing industry to continue its efforts to decrease these risks through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.").

47. The Commission did not warn businesses about the dangers of P2P networks until after it commenced action against LabMD in January 2010. (Fed. Trade Comm'n, Peer-to-Peer File Sharing: A Guide for Business, (January 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business (last accessed Aug. 9, 2015)).

48. In July, 2007, Richard E. Wallace ("Wallace") was hired by Boback and Tiversa as a forensic analyst. (Wallace, Tr. at 1337, 1339-1340).

49. Wallace prepared the materials used by Boback and Tiversa at a July 24, 2007 hearing before the United States House of Representatives Committee on Oversight and Government Reform ("OGR"), Chairman Henry Waxman presiding. (Wallace, Tr. 1341-1342).

50. Boback and Tiversa lied to Congress when Boback stated to OGR on July 24, 2007 that Tiversa's systems had obtained all files and information downloaded from P2P networks. (Wallace, Tr. 1432-1433).

49. Wallace handled "special projects" for Boback. (CX 0872 (Gormley. Dep. at 82-83)).

50. Wallace scoured P2P networks and downloaded information from the Gnutella protocol networks. (Wallace, Tr. 1340).

52. Boback instructed Wallace to "use any and all means available to find information … [e]verything from health insurance information to [] PII, Social Security numbers, basically anything that should not be out [] on these networks." (Wallace, Tr. at 1341-1342).

PUBLIC

51. "Tiversa's platform was a series of algorithms that allowed the entire peer-to-peer network to be captured not going any deeper into any computer system but just has more breadth." (Wallace, Tr. 1340).

52. Tiversa claimed that its technology enabled it view the entire P2P network and thus provide real-time, actionable information regarding sensitive file disclosures. (Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the House Comm. on Oversight Gov't Reform, 110th Cong., 20 (July 24, 2007) (written statement of Robert Boback, Chief Exec. Officer, Tiversa, Inc.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)).

53. Tiversa's "data store" was a depository of long servers containing data that is pulled in from different networks or peer-to-peer networks. (Wallace, Tr. 1371) (JUDGE CHAPPELL: "'Data store,' what does that mean?" THE WITNESS: "It is a depository of ICE long servers that as data is pulled in from different networks or peer-to-peer networks, it's stored in the data store." JUDGE CHAPPELL: "Was it something on your computer, your server at Tiversa?" THE WITNESS: "Yes. It would be accessible from a workstation at Tiversa. There are several workstations." JUDGE CHAPPELL: "And what was in the data store?" THE WITNESS: "That would be hard copies of files that were downloaded from the Gnutella network." JUDGE CHAPPELL: "This would not be where these IP addresses would be located." THE WITNESS: "Yes." JUDGE CHAPPELL: "It would be or would not be?" THE WITNESS: "It would be." JUDGE CHAPPELL: "So that was also there, where a file could be located, as well as the actual file?" THE WITNESS: "Yes.").

54. Wallace would search and download files from the P2P networks, often without using Tiversa's search platform, which were then injected or "supplemented" into Tiversa's data

PUBLIC

store. (Wallace, Tr. 1342-1343) (JUDGE CHAPPELL: "… I've heard you talk about viewing, searching and downloading. In the context of your job at Tiversa, tell me what each term means, 'downloading,' 'viewing' and 'searching.' Did you do all of these or do they mean the same thing? Tell me what they meant in the context of your work." THE WITNESS: "There were multiple positions -- or multiple activities under my position. One of them would have been, you know, using a standard, off-the-shelf peer-to-peer client, such as LimeWire or BearShare or Kazaa or Morpheus, any of those that are, you know, affiliated with the Gnutella network. I would be able to use those clients to supplement other information that Tiversa's system possibly hadn't downloaded. So it would be just another tool to supplement the information that Tiversa would have in the data store.").

55. Wallace decided what to download without a set of written parameters. (Wallace, Tr. 7-16) (JUDGE CHAPPELL: "Who made the decision of what to download?" THE WITNESS: "That would be the person sitting at the keyboard, so me." JUDGE CHAPPELL: "Did you have a set of written parameters like if you find this, you download it, or how did that work?" THE WITNESS: "No. Because it would be very difficult to know what's inside of a file prior to downloading it.").

56. Wallace worked hand-in-hand with Boback, who decided how to best "monetize th[e] information" by contacting potential targeted entities as well as existing clients about the fraudulent "spread," or proliferation, of the P2P files on the Internet. (Wallace, Tr. 1344) (JUDGE CHAPPELL: "And once you downloaded a file, what did you do with it? Did you decide that, okay, this is worth something and then you tell Mr. Boback?" THE WITNESS: "Yes." JUDGE CHAPPELL: "How did that process work?" THE WITNESS: "***Basically, I worked very closely at the time with Bob Boback. If it was something of -- significant in***

PUBLIC

nature, then I would definitely go to Bob and say this is what we have, you know, and he would make the decision at that point how to best monetize that information, whether it be giving it to a salesperson or him calling the company directly.") (emphasis added); (Wallace, Tr. at 1361) (JUDGE CHAPPELL: "***And you used the word I think 'monetize'?***" [WALLACE]: "***Yes.***" JUDGE CHAPPELL: "***Something that could be monetized?*** [WALLACE]: ***We -- early on, we were having problems at Tiversa, we were having problems selling a monitoring contract, so we started contacting individual companies when information came out, and you would be able to charge them a lesser amount than a yearlong contract, just basically a one-off to take care of that problem right then.***") (emphasis added).

57. When Wallace downloaded or "pulled down" files from P2P networks, he recorded the type of file and the file's IP address at the time of the download. (Wallace 1344-1345) (BY MR. SHERMAN: Q. "So, Mr. Wallace, when you were viewing files, is it correct to say that when you were viewing files on the network, you were not actually viewing the content of those files?" A. "***You would start out by viewing the file title, the type of file that it is, and you would record the IP and port.*** …" Q. "…***You used the term 'pull down.' Does that mean that you would download those files?***" A. "***Yes.***") (emphasis added).

49. On or about February 25, 2008, Rick Wallace, on behalf of Tiversa, downloaded a LabMD insurance aging file that was 1,718 pages in length from a LabMD workstation located in Atlanta, Georgia, at IP address 64.190.82.42. (Wallace, Tr. 1441).

50. Wallace was a uniquely skilled computer analyst, especially adept at using P2P networks, and he was engaged in a focused search to uncover commercially valuable data at the expense of unsuspecting victims. (Wallace, Tr. 1339-1391).

51. Wallace was a law enforcement asset. (Wallace, Tr. 1369, 1445).

PUBLIC

52. Wallace was hired by Boback to help generate business. (Wallace, Tr. 1344, 1360-1361, 1364).

53. Wallace acted as an instrument of and abettor for Boback and Tiversa in defrauding LabMD and Tiversa's clients. (Wallace, Tr. 1366-1367).

54. Tiversa's business model was to take files, manufacture "spread" using false IP addresses so that they appeared to be available on the Internet, and then sell "remediation" services to the victimized companies. (Wallace, Tr. 1366-1367).

55. Boback and Tiversa directed Wallace to intentionally create the illusion that companies' PII and/or PHI was widely available on P2P networks. (Wallace, Tr. 1367-1368) (Q. ***"Can you explain to us how you would make it appear as though the data had proliferated?" A. "Sure. So as we talked about earlier, if you use a stand-alone client like a LimeWire or Kazaa or BearShare or whatever you have to supplement the data store with information, there is a folder that I would direct – or that I would put files in that would show up in the data store, you know, with Coveo or whatever application you're using to have a front end. It would show up just like it was downloaded from that IP***. …") (emphasis added); (JUDGE CHAPPELL: "***Let me get this straight. … You actually did it. You actually made it available around the Internet in peer-to-peer*** — [WALLACE]: "***No. No. We would only make it appear to have been downloaded from a known bad actor. So if you have an identity thief in Arizona, say, for example, we already know law enforcement has already dealt with that individual. We know that the IP is dead. We know that the computer is long gone. Therefore, it's easy to burn that IP address because who's going to second-guess it." JUDGE CHAPPELL: "So to boil this down, you would make the data breach appear to be much worse than it actually had been." [WALLACE]: That's correct.***") (emphasis added).

PUBLIC

56. A pertinent example of the fraud committed by Boback and Tiversa is CX 0019, which is the list of IP addresses created by Wallace at Boback's specific command to make it appear as if LabMD's insurance aging file had spread or proliferated on the P2P network when in fact that was never the case. (Wallace, Tr. 1368-1370) (Q. "***I submit to you that what's on your screen has been marked as CX 19 and has been admitted into evidence in this case.***" Q." ***What is that document?***" A. "***That is a list of IP addresses that was created in the November 2013 time frame of Bob came to me and basically said that him and LabMD are having it out, there's -- I didn't really follow the whole legal proceedings, but I knew that there was some bad water there. And Bob said that under no circumstances can the insurance aging file appear to have come from a 64 IP or in the Atlanta area. These IPs that are used here, these are all identity thieves that was provided from me to Bob***. …" Q. "… ***So the purpose of creating the document in front of you was what?***" A. "***That was after Bob came to me and said that under no circumstances can the insurance aging file originate from a Georgia IP address or an Atlanta area IP address. And in addition to that, he told me to find an individual in San Diego to include with this list.***") (emphasis added).

57. The list of IP addresses on CX0019 was created by Wallace at Boback's express direction containing known criminals' IP addresses on P2P networks obtained by Wallace, as well as the date and time the file was "modified" and appended with LabMD's stolen insurance aging file, and then injected into Tiversa's data store. (Wallace, Tr. 1374-1385).

58. Wallace and Boback met with FTC officials, including but not limited to Complaint Counsel Alain Sheer, with a view towards create a wholly false document which would make it appear that LabMD's insurance aging file had spread on P2P networks, when in fact that was never the case. (Wallace, Tr. 1386-1388) (Q. ***"Who traveled to D.C. [to meet with***

PUBLIC

Alain Sheer and FTC] from Tiversa?" A. "***Bob Boback was driving. I was in the car, Anju Chopra and Keith Tagliaferri.***" Q. "***Following the meeting, did the people from Tiversa have discussions about the meeting?***" A. "***Yeah. I mean, we -- Bob spoke to me about next steps on the way home.***" Q. "***And what were the next steps?*** …" A. "***… Bob had indicated to me that the files needed to have spread on them, you know, basically look for them and see if they are available at other IP addresses, and if they're not, make them appear to have -- you know, be at different IP addresses.***") (emphasis added); (A. ***"Yes. That was the purpose of the meeting, was to clarify the – how I put the data together, how it would correspond with the list and the actual file."***) (emphasis added); (BY MR. SHERMAN: Q. ***"You testified that the purpose of the meeting was to discuss the information provided pursuant to the CID; is that correct?"*** A. ***"Yes."*** Q. ***"And do you recall who was at the meeting?"*** A. ***"There were multiple people. I mean, I don't – I don't remember specific – I do remember Alain was there."*** Q. ***"Alain who?"*** A. ***"Alain Sheer."***) (emphasis added).

59. The Commission's interest in LabMD stems from a study conducted by Dr. Eric Johnson ("Johnson"), then at Dartmouth College ("Dartmouth") and now at Vanderbilt University, "Data Hemorrhages in the Health-Care Sector," (CX 0382) and the 2009 testimony of Robert Boback before Congress – in both of these sources, the 1718 File was used as an example of a serious data breach. (RX 0403 (E. Johnson emails and article re: data hemorrhaging)); (CX 0721 (Johnson, Dep. at 68-69); (CX 0703 (Boback, Dep. at 156)).

60. Commission staff reached out to Dr. Johnson in February, 2009, and asked for a copy of the data hemorrhaging report and Dr. Johnson complied by sending them a copy. (RX 403 (E. Johnson emails and article re: data hemorrhaging)); (Johnson, Tr. 784).

61. Dr. Johnson's work largely focused on inadvertent sharing via P2P networks

PUBLIC

because these networks were used to share music, videos and pictures coupled with the fact that there is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); RX 524 (Hill, Dep. at 149)).

62. In or around January 2008, Tiversa was a research partner to Dr. Johnson and Dartmouth College in a federally-funded study of data security in the health care industry. (Johnson, Tr. at 802-804); (Daugherty, Tr. at 979-985); (Tr. at 56-58 (opening statement)).

63. Tiversa aided Dartmouth's research by obtaining business-related records, including records containing sensitive patient information belonging to health care providers, found on P2P networks and provided this information to Dartmouth for its "Data Hemorrhages" article. (Johnson, Tr. 753-755; CX 0872 (Gormley, Dep. at 55-57)).

64. Complaint Counsel has not introduced any evidence that Tiversa, Johnson or Dartmouth had permission from any person, whether listed on the 1718 File or not, to obtain or disclose PHI as required by HIPAA. (Tr. 1-1486); (CX 0001 – CX 0878).

65. In January, 2008, Tiversa, using its patented technology, conducted searches on P2P networks using Dartmouth's search terms. (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 000010)).

66. Although LabMD's 1718 File is included and discussed in Dartmouth's "Data Hemorrhages" article, Dartmouth did not obtain the 1718 File using its search terms combined with Tiversa's technology. (Johnson, Tr. 772-780); (CX 0872 (Gormley, Dep. at 98-102)).

67. In April, 2008, months after Tiversa had concluded searching using Dartmouth's search terms, Johnson requested that Gormley provide him with more recently found information that would help "spice up" and "boost the impact" of his "Data Hemorrhages" article. (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 000010); (CX 0872 (Gormley, Dep. at

PUBLIC

69-71)); (RX 483 (Emails between C. Gormley and E. Johnson Re: WSJ article); (Johnson, Tr. 772-774)).

68. The 1718 File was provided to Dartmouth as a result of Johnson's request to "spice up" and "boost the impact" of his report. (CX 0872 (Gormley, Dep. at 103); (Johnson, Tr. 779-780)).

69. Neither Tiversa nor Johnson nor Dartmouth had permission from any person listed in the 1718 File to disclose or obtain their PHI as required by HIPAA. (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5)).

70. In May 2008, Tiversa began contacting LabMD to purchase its remediation services, including sending LabMD a Tiversa Incident Response Services Agreement describing the fee schedule, payment terms, and services that would be provided – these contacts continued from mid-May through mid-July. (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (CX 0021 (Tiversa Incident Response Services Agreement); (Daugherty, Tr. 985-987)).

71. It was not until LabMD instructed Tiversa to direct any further communications to LabMD's lawyer that Tiversa ceased to press LabMD to purchase its services. (RX 059 (Email between Boyle and Tiversa re: breach); (Daugherty, Tr. at 988-990)).

72. The Chairman of the United States House Oversight and Government Affairs Committee ("OGR") commenced an investigation of Tiversa over a period of months in 2014,

PUBLIC

also exploring FTC's relationship with Tiversa. (RX 542 (June 11, 2014 OGR Letter from Issa to Ramirez); (RX 543 (December 1, 2014 OGR Letter from Issa to Ramirez)).[3]

73. OGR issued a report dated January 2, 2015 that was embargoed until after Wallace testified in open court on May 5, 2015. (RX 644 ((STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA), *available at* http://www.scribd.com/doc/265820770/2015-01-02-Staff-Report-for-Rep-Issa-Re-Tiversa#scribd (last visited Aug. 9, 2015)).

74. The Staff Investigative Report from OGR makes many notable claims apparently based on documentary evidence supporting Wallace's testimony, including the following:

- Phone records and emails subpoenaed from FTC show a working relationship between Commission Staff and Tiversa beginning in 2007, as Wallace testified. ((RX 644 ((STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56-59) (citations omitted); (Wallace, Tr. 1346-1349)).
- The Report claims that in October, 2007, Boback provided FTC with documents. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).

[3] RX 542 and RX 543 were admitted into evidence by this Court for notices purposes only on February 12, 2015.

PUBLIC

- Wallace testified to a meeting in August 2009 between Tiversa and FTC that led Boback to demand evidence of "spread." (Wallace, Tr. 1385) (Q. "Mr. Wallace, have you ever traveled to Washington, D.C. to meet with the FTC?" A. "Yes." Q. "When did you do that?" A. "I would say it would have been -- ***it would have been after the CID was issued [in July-August 2009]***, but I'm not sure of the exact date." Q. "Would it also have been after the list of companies was provided pursuant to the CID?" A. "***Yes. That was the purpose of the meeting, was to clarify the – how I put the data together, how it would correspond with the list and the actual file.***") (emphasis added); (Wallace, Tr. 1386 (BY MR. SHERMAN: Q. "You testified that the purpose of the meeting was to discuss the information provided pursuant to the CID; is that correct?" A. "Yes." Q. "And do you recall who was at the meeting?" A. "There were multiple people. I mean, I don't – I don't remember specific – ***I do remember Alain was there." Q. "Alain who?" A. "Alain Sheer."***) (emphasis added); (Wallace, Tr. 1387-1388) (Q. "Who traveled to D.C. [to meet with Alain Sheer and FTC] from Tiversa?" A. "Bob Boback was driving. I was in the car, Anju Chopra and Keith Tagliaferri." ***Q. "Following the meeting, did the people from Tiversa have discussions about the meeting?" A. "Yeah. I mean, we -- Bob spoke to me about next steps on the way home."*** Q. ***"And what were the next steps? …***" A. "… ***Bob had indicated to me that the files needed to have spread on them, you know, basically look for them and see if they are available at other IP addresses, and if they're not, make them appear to have -- you know, be at different IP addresses.***") (emphasis added).

PUBLIC

- OGR's Staff Investigation Report also claims a meeting occurred in August 2007 between FTC and Tiversa. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).
- OGR's Staff Investigation Report reproduces emails that purport to show Tiversa/Boback used advanced knowledge of FTC regulatory action for its own commercial gain, working with Lifelock to solicit business from companies that would be contacted by FTC. (RX 644 (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).
- OGR's Staff Investigation Report speculates that Tiversa could not have done so without some sort of inside knowledge of pre-decisional, non-public information. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 52, 56, 62, 67) (citations omitted)).
- OGR's Staff Investigation Report claims FTC supposedly admitted in a briefing that the use of Tiversa's information was "unusual relative to standard agency operating procedures for enforcement measures," and that it relied heavily on Tiversa's "credible" reputation in "self-verifying" the information it had provided.

PUBLIC

(RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 61) (citations omitted)).

- Wallace testified that Tiversa's Marine One claims were false and fabricated (Wallace, Tr. 1453-1454), and OGR's Staff Investigation Report makes similar claims consistent with Wallace's testimony.

  (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 16-18) (citations omitted)).

75. FTC was aware Tiversa had a clear and direct economic interest in FTC action against the companies it turned over for enforcement action. (CX 0679 (Ex. 5 (Dissenting Statement of FTC Comm'r J. Thomas Rosch, FTC File No. 1023099 (June 21, 2012)).

72. Shortly after the 2007 Congressional testimony concerning file sharing over P2P networks at which Boback and FTC Commissioner Engle testified, FTC began having frequent meetings with Tiversa to discuss its technology and the type of information that could be found on P2P networks. (Wallace, Tr. 1347-1350).

73. FTC personnel travelled to Tiversa's offices in Pittsburgh to get a demonstration of the technology. (Wallace, Tr. 1351).

74. FTC began requesting information from Tiversa that met a certain threshold which consisted of personally identifiable information exposed for greater than 100 people. (Wallace, Tr. 1562).

75. In 2009, the FTC and Tiversa agreed that a CID would be served on the Privacy Institute to funnel information from Tiversa to FTC. (RX 525 (Kaufman, Dep. at 20)).

PUBLIC

76. The Privacy Institute was the company established to accomplish this. (Wallace, Tr. 1353); (CX 0703 (Boback, Dep. at 38-41)).

77. Wallace gathered the information and prepared the list of companies to be provided to FTC in response to the CID that the FTC served on the Privacy Institute. (Wallace, Tr. 1353-1354).

78. The list Wallace provided came from Tiversa's incident response case spreadsheet which Tiversa salespeople, including Boback, would use to sell Tiversa's remediation services to companies whose information Tiversa had discovered via P2P networks. (Wallace, Tr. 1359).

79. Boback provided the FTC with the list in response to the CID to the Privacy Institute as a way to get the companies contacted by the FTC to purchase Tiversa's services. (Wallace, Tr. 1352-1353).

69. The IP address listed on exhibit CX 0307 –64.190.82.42– is LabMD's IP address. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1353-1354)).

70. Tiversa later provided CX 0019 to FTC pursuant to a subpoena served upon Tiversa in conjunction with Mr. Boback's deposition. (CX 0541 (Boback, Dep. at 22-23)).

71. Wallace provided Boback with a copy of CX 0019 within 30 days of Boback's deposition. (CX 0541 (Boback, Dep. at 22-23)).

72. At Boback's direction Wallace created CX 0019 to demonstrate spread of the 1718 File to other IP addresses, and to establish that the 1718 File had not been found and taken from LabMD's IP address. (Wallace, Tr. 1380-1385).

73. The 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

PUBLIC

74. It was not uncommon for Boback to retaliate against those who refused to purchase Tiversa's services. Boback instructed Wallace to make sure LabMD's name was at the top of the list provided to FTC. (Wallace, Tr. 1364-1366).

75. Despite Boback's testimony that Tiversa "responded to the civil investigative demand exactly to the letter," (CX 0703 (Boback, Dep. at 143)), some of Tiversa's clients who fit the criteria set out by the CID were omitted from the list. (Wallace, Tr. 1362-1363).

76. Complaint Counsel has declared it will not rely on Boback's testimony or CX 0019. (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Complaint Counsel's Opposition to Motion to Admit Select Exhibits, at 10, n.11 (June 24, 2015); (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Complaint Counsel's Response to Respondent's Motion to Refer Tiversa, Inc., Tiversa Holding Corp., and Robert Boback, at 2, n.1 (July 1, 2015)) ("As set forth in Complaint Counsel's Opposition to Respondent's Motion to Admit Select Exhibits, Complaint Counsel does not intend to cite to CX0019 or Mr. Boback's testimony in its proposed findings of fact. Nor does Complaint Counsel intend to cite to expert conclusions predicated on CX 0019 or Mr. Boback's testimony.") (citation omitted).

77. In 2009, FTC met with Tiversa to discuss the documents Tiversa provided to the Privacy Institute in response to the Civil Investigative Demand that FTC and Tiversa agreed would be served upon the Privacy Institute. (CX 0703 (Boback, Dep. at 140-142); (RX 525 (Kaufman, Dep. at 20)).

78. FTC first contacted LabMD about its investigation of LabMD in January 2010 with a telephone call to LabMD by Mr. Alain Sheer ("Sheer") and a subsequent eleven (11) page letter. (Daugherty, Tr. 992-994).

PUBLIC

79. Mr. Daugherty instructed his employees to gather all documentation requested by the letter and provide it to FTC. (Daugherty, Tr. 996-997).

80. As a result of the Commission's collaboration with Tiversa, the Commission issued a February 22, 2010, press release titled "Widespread Data Breaches Uncovered by FTC Probe." (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

81. The Commission stated: "'we found health-related information, financial records, and drivers' license and social security numbers--the kind of information that could lead to identity theft…'" and that it had "notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, ha[d] been shared from the organizations' computer networks." (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

82. The information "found" by the Commission was actually given to it by Tiversa. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX 0703 (Boback, Dep. at 141-142)).

83. Over the next 18 months there were a series of resubmissions by LabMD to the FTC as well as phone calls and meetings about whether the information submitted was responsive and sufficient. (Daugherty, Tr. 997-1001); (CX 0443 (LabMD Access Letter Response by Philippa Ellis); (CX 0444 (LabMD Access Letter Response by Philippa Ellis); (CX 0445 (LabMD Access Letter Response by Philippa Ellis); (CX 0446 (LabMD Access Letter Response by Philippa Ellis); (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld);

PUBLIC

(CX 0448 (LabMD Access Letter Response by Dana Rosenfeld); (CX 0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions)).

84. In or around August or September 2011, LabMD was presented with a Consent Decree that LabMD refused to sign. (Daugherty, Tr. 1001-1002).

85. In August, 2013, Complaint Counsel filed a Complaint and Notice Order against LabMD. (Complaint, at 12 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

D. <u>LabMD's Data Security</u>.

86. There is no perfect data security. (CX 0721 (Johnson, Dep. at 25, 38, 90); RX 524 (Hill, Dep. at 149); (Order Denying Respondent LabMD's Motion to Dismiss, at 18-19 (Jan. 16, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (last accessed Aug. 9, 2015)).

87. According to Complaint Counsel and its expert Dr. Raquel Hill ("Hill" or "Dr. Hill"), LabMD's data security was unreasonable because Respondent engaged in a number of practices between 2005 and July, 2010 that taken together failed to provide reasonable and appropriate security for personal information on its computer networks. (Complaint, at 3 ¶ 10 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

88. Dr. Hill testified that she did not consider FTC standards and guidelines for data security in determining whether LabMD's data security during the Relevant Period met those standards. (Hill, Tr. 230-231).

89. In reviewing data security standards and guidelines to assist in formulating her opinion in this case, Dr. Hill did not consider HIPAA guidelines or FTC data security standards. (Hill, Tr. 235-236); (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business

PUBLIC

(Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)) ("A sound data security plan is built on 5 key principles: 1. Take stock. Know what personal information you have in your files and on your computers. 2. Scale down. Keep only what you need for your business. 3. Lock it. Protect the information that you keep. 4. Pitch it. Properly dispose of what you no longer need. 5. Plan ahead. Create a plan to respond to security incidents.").

90. FTC's "guide" entitled Protecting Personal Information: A Guide to Business was not published in the Federal Register and was issued in November 2011, more than one year after FTC commenced its inquisition in this case. (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)).

92. During the Relevant Time the LabMD Employee Handbook advised employees of the importance of compliance with HIPAA and the "Privacy of Protected Information" and that disclosure of PHI could result in termination. (CX 0001 (LabMD Employee Handbook (rev. June 2004), at 6); (CX 0002 (LabMD Employee Handbook (rev. Mar. 2008), at 5-6)).

93. During the Relevant Time each and every LabMD employee signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement indicating that they had received the LabMD handbook and had an understanding of and would comply with LabMD's ethics policy and employment policy. (CX 0130 (LabMD Employee Handbook)).

94. At all times relevant LabMD's Employee Handbook informed employees that LabMD computers were to be used for company purposes only and prohibited personal internet

PUBLIC

or email usage. (CX 0001 (LabMD Employee Handbook (rev. June 2004), at 7); (CX 0002 (LabMD Employee Handbook (rev. Mar. 2008), at 7)).

95. Effective January 2003, LabMD had in place a Compliance Program for all employees which set forth the Policies and Standards of Conduct regarding Compliance Protocols, laws, statutes, regulations, rules and guidelines under which LabMD operated for the period 2003–2008. (CX 0005 (LabMD Compliance Program, at 1–10)).

96. Effective the Fourth Fiscal Quarter 2001, LabMD had the following Policies in practice: Data Backup Policy and Employee User Account Policy. (CX 0006 (LabMD Policy Manual, at 10, 12); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

97. Effective the Second Fiscal Quarter 2002, LabMD had the following Policies in practice: Desktop Monitoring Policy; Document Backup Software Policy; Monitor Security Software Settings and Operating System Updates Policy; Password Policy; Risk Assessment and Vulnerability Policy; Security Assignment and Accountability Policy; Server Monitoring Policy; and Software Monitoring Policy. (CX 0006 (LabMD Policy Manual, at 11, 13–19); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

98. Effective the Second and Fourth Fiscal Quarters (FQ) 2003, LabMD had the following Policies in practice: Client User Account Policy (Second FQ) and Audit Security Operations and Internet Connectivity Policy (Fourth FQ). (CX 0006 (LabMD Policy Manual, at 8–9); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

99. Effective the Second Fiscal Quarter 2004, LabMD had the following Policy in practice: Acceptable Use and Security Policy. (CX 0006 (LabMD Policy Manual, at 3–7); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

PUBLIC

100. LabMD informed all employees of "new policies that may be added to the following general employment policies and guidelines" contained in the LabMD employee handbook. (CX0001 (LabMD Employee Handbook, at 2)).

101. "Our Ethics Policy is included in the employee handbook and you will learn more about safety, privacy, security and other policies in the next several weeks of your orientation." (CX 0001 (LabMD Employee Handbook, at 2)).

102. LabMD's Mission Statement for the period 2004–2008 was as follows: "Using all reasonable means, LabMD has the intent to be fully compliant with the rules, laws and guidelines regulating its business." (CX 0001 (LabMD Employee Handbook, at 3)).

103. LabMD's Purpose for the period 2004–2008 was as follows: "LabMD, Inc. seeks to operate within the guidelines and intent of laws, statutes and regulations governing medical laboratories. In keeping employees and business associates educated, informed and trained, we can be watchful of our lab, business and billing practices in an effort to move responsibility for compliance to all levels and all departments of our organization. In short we intend to make compliance everyone's job. This compliance program establishes a formal structure to monitor, detect, respond to, and correct violations of applicable federal, state and local laws, and regulations, as well as violations of the Standards of conduct [*sic*] and LabMD policies. Our objective is to make compliance a business competency shared, valued and practiced by all individuals within LabMD. LabMD shall provide mechanisms and resources broad enough to accomplish this objective. This Corporate Compliance Program applies to all officer [*sic*], employees, business associates and agents of LabMD, Inc." (CX 0001 (LabMD Employee Handbook, at 3)).

PUBLIC

104. LabMD's Statement of Purpose and Ethics Policy for the period 2004-2008 required total compliance at all times by all employees with all applicable federal, state, and local laws, regulations and policies. (CX 0001 (LabMD Employee Handbook), at 1-23)).

105. LabMD's Corporate Compliance Program, Standards of Conduct, and Policies for the period 2004-2008 required total compliance at all times by all employees with said Program, Standards, and Policies. (CX 0001 (LabMD Employee Handbook, at 1-23)).

106. LabMD's Confidentiality and Trade Secrets Policy for the period 2004-2008 was as follows: "In the course of your work, you may have access to confidential information regarding LabMD, its suppliers, customers, operations methods, current or potential products or services and software used at LabMD. It is one of your most serious responsibilities that you in no way reveal or divulge any such information and that you use information only in the performance of your duties, as certain information could be used by competitors. . . . Removal and/or possession [of LabMD information] without . . . authorization is prohibited and subject to disciplinary action up to and including termination. . . ." (CX 0001 (LabMD Employee Handbook, at 5)).

107. LabMD's Privacy of Protected Health Information (PHI) Policy for the period 2004-2008 was as follows: "[HIPAA] made it illegal for any person in health care to share an individual's protected health care information [PHI] with anyone other than for the specific reasons of treatment, payment or health care operations. Because of this, LabMD has taken specific measures to ensure our compliance with this law. As an employee you are required to share information only with authorized individuals and only for specific, authorized reasons. You will learn more about how that affects your job specifically. Any person providing PHI to another person that is unauthorized will be disciplined up to and including termination."

PUBLIC

(CX 0001 (LabMD Employee Handbook, at 6)).

108. LabMD's Policy regarding employee use of LabMD on–site computers for the period 2004–2008 was as follows: "***Personal internet or e–mail usage in the office is prohibited. This [P]olicy stands at all times, even when an employee is on a lunch period. Computers in the office are property of LabMD and should only be used for company related reasons.***" (CX 0001 (LabMD Employee Handbook, at 7)) (emphasis added)).

109. LabMD's Policy regarding LabMD property during the 2004-2008 time period was, in relevant part, as follows: "computers and all office equipment are LabMD's property and must be maintained according to LabMD's standards, rules, and regulations." (CX 0001 (LabMD Employee Handbook, at 9)).

110. LabMD's Policy regarding Employee Health Records during the 2004-2008 time period was as follows: "Health/medical records are not included in your personnel file. These records are confidential. LabMD will safeguard them from disclosure and will divulge such information only as allowed or required by law and in accordance with HIPAA Privacy guidelines." (CX 0001 (LabMD Employee Handbook, at 12)).

111. Effective the Second Fiscal Quarter 2008, LabMD had the following Policies in practice: PC System Setup To Prevent Downloading Files From Internet Policy; Prohibit Use Of File–Sharing Software Policy; and Security Incident Response Plan. (CX 0006 (LabMD Policy Manual, at 20-22); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

112. LabMD informed all employees of "new policies that may be added to the following general employment policies and guidelines" contained in the LabMD employee handbook. (CX 0002 (LabMD Employee Handbook, at 2)).

PUBLIC

113. LabMD's Mission Statement for the period 2008-2010 was as follows: "Using all reasonable means, LabMD has the intent to be fully compliant with the rules, laws and guidelines regulating its business." (CX0002 (LabMD Employee Handbook, at 3)).

114. LabMD's Purpose for the period 2008-2010 was identical to its Purpose for the 2004-2008 time period. (CX 0002 (LabMD Employee Handbook, at 3)).

115. LabMD's Statement of Purpose and Ethics Policy for the period 2008-2010 required total compliance at all times by all employees with all applicable federal, state, and local laws, regulations and policies. (CX 0002 (LabMD Employee Handbook, at 1-22)).

116. LabMD's Corporate Compliance Program, Standards of Conduct, and Policies for the period 2004-2008 required total compliance at all times by all employees with said Program, Standards, and Policies. (CX 0002 (LabMD Employee Handbook, at 1-22)).

117. LabMD's Privacy of Protected Health Information (PHI) Policy for the period 2008-2010 was as follows: "[HIPAA] made it illegal for any person in health care to share an individual's protected health care information [PHI] with anyone other than for the specific reasons of treatment, payment or health care operations. Because of this, LabMD has taken specific measures to ensure our compliance with this law. As an employee you are required to share information only with authorized individuals and only for specific, authorized reasons. You will learn more about how that affects your job specifically. Any person providing PHI to another person that is unauthorized will be disciplined up to and including termination." (CX 0002 (LabMD Employee Handbook, at 6)).

118. LabMD's Policy regarding employee use of LabMD on-site computers for the period 2008-2010 was as follows: "Personal internet or e–mail usage in the office is prohibited. This [P]olicy stands at all times, even when an employee is on a lunch period. Computers in the

PUBLIC

office are property of LabMD and should only be used for company related reasons." (CX 0002 (LabMD Employee Handbook, at 7)).

119. LabMD's Policy regarding LabMD property during the 2008-2010 time period was, in relevant part, as follows: "[C]omputers and all office equipment are LabMD's property and must be maintained according to LabMD's standards, rules, and regulations." (CX 0002 (LabMD Employee Handbook, at 9)).

120. Effective June 1, 2010, LabMD utilized a completed Computer Hardware, Software and Data Usage and Security Policy Manual, which documented LabMD's existing policies and incorporated ongoing data security policies. (RX 0074 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual, at 1-32)).

121. For the period 2001-2010, LabMD utilized in practice the following data security policies for evaluating, identifying and addressing confidentiality and data security measures, safeguards, and risks: (1) Acceptable Use and Security Policy; (2) Assessment – Audit Policy; (3) Audit Security Operations and Internet Connectivity Policy; (4) Client User Account Policy; (5) Data Backup Policy; (6) Desktop Monitoring Policy; (7) Document Backup Software Policy; (8) Education and Training – Anti–Virus and Anti–Spyware Applications; (9) Education and Training – Instruction for Closing Network Connections; (10) Education and Training – Instruction of P2P Applications; (11) Employee User Account Policy; (12) Monitor Security Software Settings and Operating System Updates Policy; (13) Password Policy; (14) PC System Setup To Prevent Downloading Files From Internet Policy; (15) Prohibit Use of File–Sharing Software Policy; (16) Risk Assessment and Vulnerability Policy; (17) Security Assignment and Accountability Policy; (18) Security Incident Response Plan; (19) Server Monitoring Policy; and (20) Software Monitoring Policy. (CX 0445 (LabMD Access Letter Response by Philippa Ellis);

PUBLIC

(RX 074 (LabMD Computer Hardware and Security Manual, at 1-32); (CX 0006 (LabMD Policy Manual, at 1-22); (CX 0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual at 2, 11-32)).

122. Information in LabMD's Employee Handbook qualifies as the written policies of the company. (Hill, Tr. 289).

123. In 2001, LabMD hired an IT consulting firm, ITrain Tech, to design and set up LabMD's IT system at its Savannah, Georgia location. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

124. For LabMD, ITrain Tech focused on the design and implementation of IT networks and PC setup projects primarily for small businesses and assisted with network design, including the purchase and installation of software and firewalls. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

125. ITrain Tech was under contract with LabMD through August 2004 and remained on call as necessary thereafter. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

126. LabMD IT employee Jeremy Dooley ("Dooley") started with the company in 2004 and ended his employment in December, 2006. He testified that during his tenure LabMD had firewalls installed to protect against intrusions, as well as antivirus software. (CX 0711 (Dooley, Dep. at 31, 71-72)).

127. Dooley signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement on March 10, 2005. (CX 0130 (LabMD Employee Handbook, at 003835)); (CX 0711, (Dooley, Dep. at 143)).

PUBLIC

128. Dooley's first title and responsibilities were as the communication coordinator assigned with calling insurance companies to verify benefits. (CX 0711 (Dooley, Dep. at 13)).

129. Later Dooley joined the technical support team and would go around and repair computers. (CX 0711 (Dooley, Dep. at 15- 16)).

130. Lytec was the billing software used by LabMD. (CX 0711 (Dooley, Dep. at 52-53)).

131. LabSoft was the laboratory software used by LabMD. (CX 0711 (Dooley, Dep. at 125)).

132. At that time, LabMD had firewalls installed to protect against intrusions and also installed antivirus software. (CX 0711 (Dooley, Dep. at 31, 71-72)).

133. Both the lab software and the billing software had separate firewall routers. (CX 0711 (Dooley, Dep. at 24)).

134. Security risks and vulnerabilities were assessed by Automated PC Technologies ("APT"), an outside contractor. (CX 0711 (Dooley, Dep. at 38-39)).

135. Allen Truett ("Truett") started APT in 1996 – APT provided technology consulting services to small and medium-size businesses. (CX 0731 (Truett, Dep. at 17-18)).

136. APT began providing services to LabMD in 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX 0731 (Truett, Dep. at 25, 72-73)).

137. APT consulted with and made recommendations to LabMD with respect to installing and maintaining firewalls and antivirus software to mitigate threats and risks for medical organizations like LabMD to prevent information on its secure internal network from being accessed from the outside. (CX 0731 (Truett, Dep. at 45-46)).

PUBLIC

138. APT performed network diagnostics by looking at network traffic. (CX 0711 (Dooley, Dep. at 52); (CX 0731 (Truett, Dep. at 69)).

139. APT installed and managed antivirus software. (CX 0711 (Dooley, Dep. at 71-72); (CX 0731 (Truett, Dep. at 19)).

140. APT provided backup software and applied patches. (CX 0711 (Dooley, Dep. at 114); (CX 0731 (Truett, Dep. at 32)).

141. APT was an IT outsourcing company specializing in the medical field. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

142. APT's start-up procedures for LabMD included an evaluation its antivirus and firewall systems. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld (Ex. 3)).

143. APT began evaluating LabMD's existing security features and providing backup services to LabMD, including identifying and remedying a problem with LabMD's server's virus scan on May 3, 2006. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld (Ex. 5)).

144. APT identified and resolved anti-virus program concerns at LabMD throughout 2006. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld)).

145. After advising LabMD to install an additional firewall on May 6, 2006, APT obtained LabMD's authorization and delivered the new firewall for installation on May 12, 2006. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld (Ex. 5)).

146. APT implemented and tested all new upgrades during the period of August 2003 through March 2007 to ensure that equipment and software was functioning properly. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld (Ex. 4)).

PUBLIC

147. APT installed a ZyWALL firewall application, which was specific to APT's medical clients for Internet security, and another firewall application for LabMD during the 2006-2008 time period. (CX 0731 (Truett, Dep. at 31, 33, 41)).

148. During the 2006-2008 time period, APT did work concerning the administration of servers and firewalls and "[i]nstallation of service packs and upgrade and software patches for PCs and servers." (CX 0731 (Truett, Dep. at 31-33)).

149. On May 12, 2006, APT delivered a ZyWALL 5 IPSec firewall to LabMD. (CX 0731 (Truett, Dep. at 60-61)).

150. During the period 2006-2008, LabMD installed and utilized Trend Micro antivirus software. (CX 0731 (Truett, Dep. at 89)).

151. During the period 2007-2008, LabMD had Veritas backup software on its servers. (CX 0724 (Maire, Dep. at 23)).

152. During the period 2007-2008, ClamWin was the antivirus software installed on LabMD's client's computers. (CX 0724 (Maire, Dep. at 95)).

153. During the period 2007-2008, LabMD had a Windows firewall on its computer system. (CX 0724 (Maire, Dep. at 97)).

154. LabMD's computer data security was reasonable and appropriate for the period 2007–2008. (CX 0724 (Maire, Dep. at 89)).

155. LabMD had a firewall intrusion-prevention system in place for the period 2007-2008. (CX 0724 (Maire, Dep. at 91)).

156. LabMD had in place the Zywall firewall hardware and other security measures, including Internet access restrictions for non-managerial employees, as well as TrendMicro anti-virus software and stratified profile setups, which limited the ability of employees to modify

PUBLIC

computer settings and which were organized at three different levels: "Admin," "Local Admin," and "User level," for administrators, managers and line-level employee users). (CX 0704-A (Boyle, Dep. at 49-55)).

157. At the time, IT support services were provided by APT and internal staffing, and LabMD IT personnel implemented network upgrades and maintained the day-to-day monitoring and functioning of the network. (CX 0704-A (Boyle, Dep. at 12, 39, 44-48)).

158. There were layers of authentication with the initial layer being the Windows network and the others being a layer for the billing software and a layer for the lab software. (CX 0711 (Dooley, Dep. at 125)).

159. LabMD placed restrictions on employees' access to information through the authentication layers, usernames and passwords. (CX 0711 (Dooley, Dep. at 124-127)).

160. Only certain individuals were given administrator user profiles which gave them the ability to install applications. Most employees were given standard user profiles. (CX 0711 (Dooley, Dep. at 47-49)).

161. Dooley had no concerns about the security of LabMD's network. (CX 0711 (Dooley, Dep. at 151-152)).

162. There were no concerns about the security of LabMD's network either specifically or generally, and there were no incidents of unauthorized access. (CX 0731 (Truett, Dep. at 126-127)).

163. Outside contractors were brought in proactively to identify security issues. (CX 0711 (Dooley, Dep. at 152)).

164. Billing employee Nicotra Harris ("Harris") was employed by LabMD from October 2006 through January 2013. (CX 0716 (Harris, Dep. at 11)).

PUBLIC

165. Harris described her access to the Internet as limited to insurance companies' websites or otherwise being blocked. (CX 0716 (Harris, Dep. at 82-83)).

166. Harris testified that on a yearly basis LabMD employees received training on LabMD compliance standards, HIPAA compliance, and the limited use of computer systems, including the restricted use of the Internet and the prohibition against playing CDs or downloading of information from the Internet. (CX 0716 (Harris, Dep. at 62)).

167. Harris testified that LabMD had in place user names and passwords for billing department employee computers with separate and different user names and passwords for the Lytec billing system. (CX 0716 (Harris, Dep. at 67-68)).

168. Harris testified only billing personnel could access the Lytec billing system. (CX 0716 (Harris, Dep. at 75)).

169. Harris testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. (CX 0716 (Harris, Dep. at 72-74)).

170. Harris testified insurance aging reports were created and printed by the billing managers, and that the pages were divided amongst the billing department employees for the purpose of contacting insurance companies to collect unpaid balances – when they were finished using the portion of the report they had been given they would shred them. (CX 0716 (Harris, Dep. at 34-41)).

171. Harris testified that she had no knowledge of a breach of LabMD's system during her tenure. (CX 0716 (Harris, Dep. at 130-131)).

172. Billing employee [redacted] was employed by LabMD from 2007 through January 2009. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 13)).

PUBLIC

173. [redacted] also testified to LabMD's security policies and practices including the shredding of the insurance aging reports. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 43, 45-47, 49-50, 54-55, 61-62, 65-66)).

174. [redacted] testified that she received HIPAA training by watching a video on privacy concerns and HIPAA violations. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 86)).

175. [redacted] testified that LabMD had in place user names and passwords for billing department employee computers and separate and different user names and passwords for the Lytec billing system as well as different user names and passwords for access to the LabSoft program. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 43, 45)).

176. [redacted] testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to bill denials of coverage for medically necessary tests. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 46-47)).

177. [redacted] testified insurance aging reports were created and printed by the billing managers and used for the purpose of contacting insurance companies to collect unpaid balances. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 49-50)).

178. [redacted] testified that when they were finished using the portion of the report they had been given they would shred them. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 54-55)).

PUBLIC

179. LabMD billing employee Sandra Brown ("Brown") was the billing manager from May 2005 to May 2006. (CX 0706 (Brown, Dep. at 6-7)).

180. Brown testified that from 2006 through 2013 she worked from home doing billing from insurance aging reports. (CX 0706 (Brown, Dep. at 7)).

181. Brown testified that LabMD limited internet access to the insurance company web sites and only managers had access to Microsoft Outlook emails. (CX 0706 (Brown, Dep. at 115, 121)).

182. Brown testified that non-manager billing employees did not have the same access to Lytec as the managers had, because the non-manager employees could not print reports. (CX 0706 (Brown, Dep. at 113-114)).

183. Brown testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to send information to insurance companies if they asked for medical records and for an appeals request. (CX 0706 (Brown, Dep. at 117-118, 153)).

184. Brown testified that Insurance aging report pages were shredded. (CX 0706 (Brown, Dep. at 143-144)).

185. Billing employee Patricia Gilbreth ("Gilbreth"), who later became a billing manager, was employed from 2007 to 2013 at LabMD. (CX 0715-A (Gilbreth, Dep. at 77-78)).

186. Gilbreth testified there was annual training at LabMD about HIPAA and protecting information. (CX 0715-A (Gilbreth, Dep. at 77-78)).

187. Gilbreth testified that she conducted training for new billing department employees which included the employee handbook and security handbook. (CX 0715-A (Gilbreth, Dep. at 81-83)).

PUBLIC

188. Gilbreth testified that the ability to create or print an insurance aging report was limited to a few people in the billing department. (CX 0715-A (Gilbreth, Dep. at 33-35)).

189. Gilbreth testified the aging reports were shredded. (CX 0715-A (Gilbreth, Dep. at 14-16)).

190. Gilbreth testified there were restrictions on access to the internet and there was a prohibition in the employee handbook against downloading from the internet. (CX 0715-A (Gilbreth, Dep. at 63-65)).

191. Gilbreth testified she was familiar with portions of the LabMd policy manual and the "IT security handbook" which was updated periodically. (CX 0715-A (Gilbreth, Dep. at 85-86); (CX 0006 (LabMD Policy Manual)).

192. Gilbreth testified there was a policy against personal email accounts. (CX 0715-A (Gilbreth, Dep. at 57)).

193. Gilbreth testified that she considered the downloading of LimeWire on Woodson's computer a company security policy violation. (CX 0715-A (Gilbreth, Dep. at 67-68)).

194. Gilbreth testified she had no concerns and knew of no other employee who had concerns about LabMD's information security policies and procedures. (CX 0715-A (Gilbreth, Dep. at 67)).

195. John Boyle ("Boyle") was employed as LabMD's Vice President of Operations and General Manager from November 2006 to August 2013. (CX 0704-A (Boyle, Dep. at 7-8)).

196. Boyle brought to LabMD an enormous amount of knowledge and experience in information technology and data security within the medical laboratory industry: prior to joining LabMD Boyle worked for Cyto Diagnostics as a lab technician creating slides for urine samples,

PUBLIC

a DNA analysis lab technician creating computer generated reports and was promoted to team lead responsible for the entire process from receiving and processing the samples, staffing, writing and implementing policies and procedures and processes to qualify. (CX 0704-A (Boyle, Dep. at 92-96)).

197. When Cyto Diagnostics changed its name to UroCor, Boyle became the Accessioning Manager where he was responsible for receiving the samples either electronically or hard copy, applying the verification process ensuring patient data matches the sample and the appropriate testing is ordered before processing them through to the next department. As manager Boyle wrote the procedures for UroCor electronic accessioning process requiring interaction and coordination with operations, billing, finance, sales and pathology. (CX 0704 (Boyle, Dep. at 97-100)).

198. Boyle was then promoted to the position of client relations interface manager where he interacted with the internal clients, the departments, and external clients, the physicians. (CX 0704-A (Boyle, Dep. at 101-102)).

199. Later Boyle was promoted to the position of operations business analyst where he worked daily with the IT department on applications and structure to develop working product for segments of operations. (CX 0704-A (Boyle, Dep. at 103-104)).

200. Boyle was then moved into the IT department where he became the business analyst/information planning manager where part of his duties were to choose and implement a new billing and laboratory system giving consideration to that new system's ability to receive and process information electronically. (CX 0704-A (Boyle, Dep. at 105-109)).

PUBLIC

201. At that time Robert Hyer ("Hyer") was director of IT at UroCor, and was a mentor to Boyle – both worked together at UroCor in choosing the new billing and laboratory systems for UroCor. (CX 0719 (Hyer, Dep. at 17); (CX 0704-A (Boyle, Dep. at 110-111)).

202. When UroCor was purchased by DIANON and as a result Boyle became the Oklahoma City facility laboratory manager responsible for lab management over all departments in the facility while working with the IT departments for LabCorp and DIANON which involved planning, design review, coordination between IT departments and clients and interfaces. (CX 0704-A (Boyle, Dep. at 112-113)).

203. From 2003-2006, Boyle was the director of operations for DIANON in 2003 through 2006 at which time external and internal transfers of protected health information were mostly conducted electronically and Boyle had the responsibility to ensure that those transfers were secure. (CX 0704-A (Boyle, Dep. at 114-118)).

204. When Boyle joined LabMD in November of 2006 he described LabMD's system as being designed from the outside in making it efficient for the physicians to use. (CX 0704-A (Boyle, Dep. at 123-125)).

205. Boyle found the design of the transfer of information from clients to LabMD and the internal transfer of information within LabMD to be efficient and secure. (CX 0704-A (Boyle, Dep. at 125)).

206. Information came to LabMD from physicians through a secure connection. (CX 0704-A (Boyle, Dep. at 13)).

207. Boyle assumed oversight of compliance training for LabMD employees. LabMD's existing policies already prohibited employees, other than certain authorized IT

PUBLIC

personnel, from downloading programs or applications from the Internet. (CX 0704-A (Boyle, Dep. at 39-48, 54-55, 68 -71)).

208. When Boyle arrived LabMD's IT department was flat – there were no supervisors. (CX 0704-A (Boyle, Dep. at 52-53)).

209. IT personnel (including Curt Kaloustian, Alison Simmons and Chris Maire) reported directly to Boyle. (CX 0704-A (Boyle, Dep. at 12)).

210. Upon Boyle's arrival he found that LabMD had in place the Zywall firewall application installed by APT which was specific to APT's medical clients for Internet security; along with security measures, including Internet access restrictions for non-managerial employees, TrendMicro anti-virus software and stratified profile setups, which limited the ability of employees to modify computer settings (there were three different levels: "Admin," "Local Admin," and "User level," for administrators, managers and line-level employee users). (CX 0731 (Truett, Dep. at 31, 33, 41); (CX 0704-A (Boyle, Dep. at 49-55)).

211. APT would regularly be on site at LabMD managing networking, servers, hardware and applications. (CX 0704-A (Boyle, Dep. at 47-48); (CX 0731 (Truett, Dep. at 32)).

212. IT support services were provided by APT and internal staffing, and LabMD IT personnel implemented network upgrades and maintained the day-to-day monitoring and functioning of the network. (CX 0704-A (Boyle, Dep. at 12, 39, 44-48)).

213. Boyle implemented a review of LabMD's processes and procedures, including auditing the LabMD Administration department records and ensuring that all employees for whom there was not a signed acknowledgement document on file submitted a signed document acknowledging having read LabMD's Employee Handbook or Compliance policies. (CX 0704-A (Boyle, Dep. at 71, 148)).

PUBLIC

214. Beginning in 2007, Boyle assumed oversight of compliance training for LabMD employees. LabMD's existing policies already had prohibited employees, other than certain authorized IT personnel, from downloading programs or applications from the Internet. (CX 0704-A (Boyle, Dep. at 39-48, 54-55, 68 -71)).

215. In August, 2007, LabMD implemented daily IT "walk arounds" to review the IT functions in all LabMD departments and, during the daily walk arounds, IT personnel visited each department daily and inquired if computers or computer accessories, such as printers, were showing any problems or errors. (CX 0704-A (Boyle, Dep. at 73)).

216. If a problem were reported or observed, LabMD's IT personnel would attend to it immediately, on site. (CX 0704-A (Boyle, Dep. at 39-48, 54-55, 68-71)).

217. On February 25, 2008, Rick Wallace entered LabMD's system without authorization and downloaded the 1718 File from a LabMD workstation that was running a P2P file sharing program. (Wallace, Tr. 1441).

218. Wallace entered LabMD's system without authorization and downloaded the 1718 File for Tiversa's financial benefit. (Wallace, Tr. 1344, 1360-1361, 1364).

219. At the time Wallace entered LabMD's system without authorization and downloaded the 1718 File on February 25, 2008, Georgia law provided as follows:

- **(a)** ***Computer theft.*** Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

  (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

  (2) Obtaining property by any deceitful means or artful practice; or

PUBLIC

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

- **(b)** ***Computer Trespass.*** Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

  (1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

  (2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

  (3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

- **(c)** ***Computer Invasion of Privacy.*** Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

- **(d)** ***Computer Forgery.*** Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had

PUBLIC

created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

- **(e)** ***Computer Password Disclosure.*** Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.
- **(f)** ***Article not Exclusive.*** The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this article.
- **(g)** ***Civil Relief; Damages.***

  (1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits and victim expenditure.

PUBLIC

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

- **(h)** ***Criminal Penalties.***

  (1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

  (2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

PUBLIC

(Off. Code of Ga. Ann. § 16-9-93 (2008) (Georgia Computer Crimes Statute), *available at* http://law.justia.com/codes/georgia/2010/title-16/chapter-9/article-6/part-1/16-9-93 (last accessed Aug. 9, 2015).

220. At the time Wallace entered LabMD's system without authorization and downloaded the 1718 File, HIPAA prohibited Tiversa from obtaining or disclosing PHI of any individual without that person's express permission because LabMD was a covered entity under 42 U.S.C. § 1320d-9(b)(3). (42 U.S.C. § 1320d-6(a) & (b) (Wrongful disclosure of individually identifiable health information)).

218. "The FTC's Complaint in [this] Enforcement Action makes clear that LabMD was a 'health care provider' and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 12 ¶ 42)).

218. 42 U.S.C. § 1320d-6 (a) & (b) provide as follows:

- **(a) Offense**

  A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) ***obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–***

PUBLIC

9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.

- **(b) Penalties**

A person described in subsection (a) of this section shall—(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and ***(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.***

(emphasis added).

221. There is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); (RX 524 (Hill, Dep. at 149)).

222. In May, 2008, Tiversa, through Boback, contacted LabMD alleging that the 1718 File had been found on the internet and offering "remediation" services. (RX 050 (Email between Boyle and Tiversa); (RX 051 (Email between Boyle and Tiversa); (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa) ([Boback to Boyle 15 May 2008] ("Per Rick's email below, it would require some time to get to that type of information which would need to be handled through our Incident Response Operation Team and would require a professional services arrangement. As I mentioned in my last email, there are many more necessary benefits to a proper investigation of the disclosure by our team."); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and

PUBLIC

Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (CX 0021 (Tiversa Incident Response Services Agreement); (Daugherty, Tr. 979-993)).

223. This was after Tiversa had shared the 1718 File with Johnson and Dartmouth. (CX 0872 (Gormley, Dep. at 86-87)).

224. At all times relevant, Tiversa knew or should have known the 1718 File contained highly confidential information and that it was not authorized to obtain or disclose the 1718 File to any third party because Tiversa "found" the LabMD 1718 page document, and a Tiversa email dated April 17, 2008 categorizes how many social security numbers (SSNs) and other identifying information were in that file, which included information commonly known as PII and PHI. (CX 0872 (Gormley, Dep., at 81-83, 86-87)) ("[This is] an E-mail describing the contents of a file labeled subject, LabMD disclosure, categorizing how many social security numbers and other identifying information … [MR. SHERMAN:] So it's a possibility that the LabMD disclosure as it is called in the subject line of this E-mail was discovered as a result of searches that Tiversa was doing for other clients. [Mr. Gormley:] That's possible. Social security number would have been a term that we would have looked for. CIGNA would have been a term that we would have looked for because they were a client.") (discussing Gormley Dep. Ex. RX 5 (4/17/2008 Wallace email to Gormley – subject line of "LabMD disclosure")).

221. This type of information uncovered by Tiversa would be regularly shared with Tiversa's customers. (CX 0872 (Gormley, Dep. at 83, 86-87)).

222. After Tiversa contacted LabMD, and advised that the 1718 File had been downloaded via a P2P file sharing program, at Boyle's direction, LabMD IT employee Alison Simmons ("Simmons") searched all computers at LabMD for file sharing software. (CX 0704 (Boyle, Dep. at 57-66, 74-88); (CX 0149 (Screenshot: LabMD - Tiversa.zip WINRAR -

PUBLIC

insuranceaging_6.05.071.pdf); (CX 0150 (Screenshot: C:\); (CX 0151 (Screenshot: C:\Program Files\LimeWire); (CX 0152 (Screenshot: LimeWire: My Shared Files); (CX 0153 (Screenshot: LabMD - Tiversa.zip WinRAR - LabMD folder); (CX 0154 (Screenshot: LimeWire Get Started); (CX 0155 (Screenshot: Start Menu: LimeWire); (CX 0156 (Screenshot: LimeWire: Options: Shared Folders); (CX 0157 (Screenshot: insuranceaging_6.05.071.pdf Properties)).

223. Simmons found no file sharing software on any other computer except for the billing manager Roz Woodson's computer. (CX 0730 (Simmons, Dep. at 10-11)).

224. Simmons removed the LimeWire file sharing program from Woodson's computer. (CX 0730 (Simmons, Dep. at 14-15)).

225. According to Simmons the billing department had a firewall and billing employees were prohibited from going to nonspecified web sites, except for those needed to perform their jobs. (CX 0730 (Simmons, Dep. at 16)).

226. Under Boyle's supervision and with his personal assistance, LabMD IT personnel Simmons and Jeff Martin ("Martin") immediately undertook a search of all other computers in the office and determined that no other LabMD computers contained either the LimeWire application or the 1718 File. (CX 0704-A (Boyle, Dep. at 57-64)).

227. To verify what LabMD had been told by Tiversa, Boyle instructed Simmons to search for the file on P2P networks from her home computer; Simmons searched for the file two hours on the day of the call from Tiversa and then once a week for a month or longer but was never able to find the 1718 file. (CX 730 (Simmons, Dep. at 17-18)).

228. As part of LabMD's investigation after the LimeWire discovery, Simmons, under Boyle's supervision, took a series of screenshots from the billing manager's computer and placed them on a CD, and the screenshots showed the date LimeWire files had been installed on the

PUBLIC

billing manager's computer and the presence of the file, which Tiversa had told LabMD it had downloaded from a P2P file sharing site. (CX 0704-A (Boyle Dep. at 57-66, 74-88)); (CX 0149 (Screenshot: LabMD - Tiversa.zip WINRAR - insuranceaging_6.05.071.pdf); (CX 0150 (Screenshot: C:\); (CX 0151 (Screenshot: C:\Program Files\LimeWire); (CX 0152 (Screenshot: LimeWire: My Shared Files); (CX 0153 (Screenshot: LabMD - Tiversa.zip WinRAR - LabMD folder); (CX 0154 (Screenshot: LimeWire Get Started); (CX 0155 (Screenshot: Start Menu: LimeWire); (CX 0156 (Screenshot: LimeWire: Options: Shared Folders); (CX 0157 (Screenshot: insuranceaging_6.05.071.pdf Properties)).

229. Boyle assigned IT employee Simmons and later Martin to search P2P networks to find the 1718 file and they could not find the file on any P2P networks. (CX 0704-A (Boyle, Dep. at 63-64)).

230. Simmons was asked to interview Woodson and determine her knowledge of the program. Simmons concluded Woodson appeared to have no idea what the program was or whether she had shared files. (CX 0730 (Simmons, Dep. at 12, 93)).

231. According to Simmons no one was supposed to download anything without going through IT. (CX 0730 (Simmons, Dep. at 17)).

232. Woodson was terminated as a result of the P2P incident. (CX 0730 (Simmons, Dep. at 99- 100)).

233. From August 2008 until June 2010 John Boyle personally conducted walk arounds on a weekly basis, assisted by Hyer or another IT employee, such as Matt Bureau ("Bureau"). (CX 0704-A (Boyle, Dep. at 39-40, 130-31)).

234. LabMD routinely performed daily IT rounds to check on the data security status

PUBLIC

of all computer systems. (RX 174 – RX 264 (LabMd Email re: Daily IT Rounds); (CX 0236 (LabMd Email re: Daily IT Rounds); (CX 0199 (LabMd Email re: Daily IT Rounds)).

235. From August, 2008, until June, 2010, Boyle and LabMD IT professionals physically reviewed each computer for the following: (1) the presence, function and updates of the TrendMicro security software; (2) MS Windows firewall security function and setup; (3) the profile set-up on each computer; (4) the installation and function of Windows security updates; (5) events recorded in the Event Viewer on the computer for errors in applications or function; (6) Internet Explorer history and use; (7) the deletion of temporary files in Internet Explorer, if applicable; (8) access to the correct network applications and servers; and, (9) Add/Remove programs to review the applications present on each computer. Through this process, LabMD checked the applications installed on each computer and verified that neither file-sharing applications, nor other unauthorized programs were on any LabMD employee's computer. (CX 0704-A (Boyle, Dep. at 43-51, 70-71)).

236. LabMD hired Hyer as the IT Manager in August, 2009, at which time IT personnel began reporting to Hyer *and* Boyle, with Hyer reporting directly to Boyle as his immediate supervisor. (CX 0704-A (Boyle, Dep. at 12)).

237. Hyer was previously the director of IT at UroCor, and was a mentor to Boyle – both worked together at UroCor in choosing the new billing and laboratory systems for UroCor. (CX 0719, (Hyer Dep. at 17); (CX 0704-A (Boyle Dep. at 110-111)).

238. When Boyle hired Hyer to work for LabMD from June 2009 to March 2012, Hyer signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement on August 24, 2009. (CX 0719 (Hyer, Dep. at 143); (CX 0130 (LabMD Employee Handbook, at 003847)).

239. Upon arrival Hyer found that Curt Kaloustian ("Kaloustian") was not qualified in

PUBLIC

any way to meet the demands of his position with LabMD. (CX 0719 (Hyer, Dep. at 41 -42)).

240. LabMd was using TrendMicro or Symantec antivirus software. (CX 0704-A (Boyle, Dep. at 43)).

241. TrendMicro was an overall security system with antivirus protection as one of its functions. LabMD had in place the current version of TrendMicro on its servers and desktops while it was in use during Hyer's tenure. (CX 0719 (Hyer, Dep. at 164 -165)).

242. The system was set up to limit access of physicians to their patients' information only. (CX 0719 (Hyer, Dep. at 142)).

243. TrendMicro created reports and staff reviewed them. (CX 0704-A (Boyle, Dep. at 46)).

244. Antivrus software was used on servers and workstations. (CX 0704-A (Boyle, Dep. at 48)).

245. LabMD had in place firewalls, routers, and Websense to protect its network. (CX 0704-A (Boyle, Dep. at 49)).

246. LabMD established policies regarding employees' passwords and access to information as there were controls by department, by function involving both lab and billing. (CX 0704-A (Boyle, Dep. at 148-149)).

247. In May, 2010, LabMD retained Providyn, Inc. to conduct quarterly scans of LabMD's servers and network which were designed to search for and detect vulnerabilities in applications or in the network that could constitute a security threat. (CX 0704-A (Boyle, Dep. at 34-41); (CX 0044 (Providyn Service Solutions Proposal for LabMD, executed by M. Daugherty)).

PUBLIC

248. Under Hyer's direction LabMD addressed and resolved the critical risk items on the Providyn vulnerability scan assessments. (CX 0719 (Hyer, Dep. at 108 -110)).

249. Hyer did not believe that a high priority item on the Providyn vulnerability scan assessment does not equate to a high probability of that risk occurring. (CX 0719 (Hyer, Dep. at 110 -111)).

250. During Hyer's tenure there were no security leaks or data breaches of point to point information being transferred between LabMD and its physician clients – scans of desktops were being run on a daily basis; the security of the servers were tested on a weekly basis. (CX 0719 (Hyer, Dep. at 156 -157)).

251. After June 2010, and as defined in the desktop monitoring policy, all computers were monitored using a defined LabMD checklist**,** and were recorded upon a monthly basis by a Desktop Technician at LabMD. If the technician was providing support for any issue, including adding a printer or performing unscheduled maintenance on a computer, the technician reviewed the entire computer, including applications on the computer, to ensure that the computer's security was functioning in compliance with LabMD policies and procedures. (CX 0704-A (Boyle, Dep. at 63-66, 68-70)).

252. In July 2010, Boyle began conducting annual training on LabMD's Policy Manual, which memorialized policies previously in place at LabMD, including the prohibition on downloading files or software from the Internet. All LabMD employees were required to attend training on the Policy Manual. Each page of the manual was initialed by each person and each employee signed the signature page. Training records were maintained by the Administration department at LabMD. (CX 0704-A (Boyle, Dep. at 68-70)).

PUBLIC

253. LabMD IT employee Christopher Maire ("Maire") started with LabMD in mid-2007 and left in mid-2008. (CX 0724 (Maire, Dep. at 10)).

254. Maire possessed a Bachelor's degree in Information Technology. (CX 0724 (Maire, Dep. at 106)).

255. According to Maire's testimony, during his tenure LabMD had written information security policies, employee handbook, HIPAA compliance and prohibition against personal use of company equipment during his tenure. (CX 0724 (Maire, Dep. at 18-19)).

256. As part of his employment Maire routinely performed daily IT rounds to check on status of all computer systems. (RX 174 – RX 264 (LabMd Email re: Daily IT Rounds); (CX 0236 (LabMd Email re: Daily IT Rounds); (CX 0199 (LabMd Email re: Daily IT Rounds); (CX 0724 (Maire, Dep. at 59)).

257. During Maire's tenure LabMD also had written policies on, audit security operations, internet connectivity policy, monitor security software settings, and operating systems updates. (CX 0006 (LabMD Policy Manual, at 8, 10, 13); (CX 0724 (Maire, Dep. at 21-23)).

258. LabMD had a firewall intrusion-prevention system in place for the period 2007-2008. (CX 0724 (Maire, Dep. at 91)).

259. During the period 2007-2008, ClamWin was the antivirus software installed on LabMD's client's computers. (CX 0724 (Maire, Dep. at 95)).

260. During the period 2007-2008, LabMD had Windows antivirus software installed on its computer system. (CX 0724 (Maire, Dep. at 97)).

261. Maire was not aware of any breach or occurrence of access to information by individuals not authorized to access such information. (CX 0724 (Maire, Dep. at 63-64)).

PUBLIC

262. LabMD provided all necessary compliance training regarding the "rules, laws and guidelines regulating its business," including, but not limited to, HIPAA and HITECH for the period January 2003 to August 2013. (CX 0005 (LabMD Compliance Program, at 1, 2-10); (CX 0127 (LabMD Compliance Training, at 1-28)).

263. Lou Carmichael ("Carmichael"), Compliance Program Manager for LabMD, created the LabMd Compliance Manual and Compliance Training in use for the relevant time period. (CX 0005 (LabMD Compliance Program, at 1–10); (CX 0127 (LabMD Compliance Training, at 1-28); (CX 0708 (Carmichael, Dep. at 26-33)).

264. HIPAA's Security Rule, Privacy Rule, and extant protections for PHI were part of LabMD's Compliance Program and Compliance Training for the relevant time period in this case. (CX 0708 (Carmichael, Dep. at 45-46)).

265. LabMD's Compliance Programs "included regular training on topics including HIPAA, Privacy and Security Regulations." (CX 0708 (Carmichael, Dep. at 54)).

266. LabMD ran virus scans on its systems. For example, during the period June 2010-July 2010, LabMD ran full virus scans daily on the following systems and/or servers: mapper server; demographics server; LabNet; specialty; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart); (RX 267 (LabMD Server Room Security Chart)).

267. LabMD ran manual scans and ensured RealTime Scanning was active on its systems. For example, during the period June 2010-July 2010, RealTime scanning was active on all LabMD computer systems and/or machines and additional manual scans were initiated as needed. (RX 266 (LabMD Server Room Security Chart); (RX 267 (LabMD Server Room Security Chart)).

PUBLIC

268. On June 11, 2010, LabMD utilized Regular Cleaner, TrendMicro, and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart)).

269. On June 11, 2010, LabMD utilized Regular Cleaner, TrendMicro, and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; specialty; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart)).

270. LabMD used Malwarebytes software on its systems. For example, on the following dates, LabMD utilized Malwarebytes software on the designated systems and/or servers: Mapper Server (June 2& 11, 2010); Demographics Server (June 10-11 & 19, 2010); LabNet (June 4 & 11, 2010); Specialty, HL7/LabCorp, and Automate (June 11, 2010); Supply Orders/Sales Reports (June 1 & 11, 2010); Lytec (June 11, 2010); Visnetic–Email (June 1, 11-12, 14, & 23, 2010). (RX 266 (LabMD Server Room Security Chart)).

271. LabMD used Regular Cleaner and Security Check software on its systems– for example, on July 5, 2010, LabMD utilized Regular Cleaner and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 267 (LabMD Server Room Security Chart)).

272. LabMD used TrendMicro on its systems – for example, on July 22, 2010, LabMD utilized TrendMicro software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Visnetic–Email. (RX 267 (LabMD Server Room Security Chart)).

PUBLIC

273. LabMD used Malwarebytes software on its systems – for example, on thefollowing dates, LabMD utilized Malwarebytes software on the designated systems and/or servers: Mapper Server (July 5, 7, 22, 26 & 29, 2010); Demographics Server (July 1, 5, 14 & 22, 2010); LabNet, Specialty, HL7/LabCorp, Automate, and Supply Orders/Sales Reports (July 5 & 22, 2010); Lytec (July 5, 2010); Visnetic-Email (July 5, 22 & 31, 2010). (RX 267 (LabMD Server Room Security Chart)).

E. <u>Fisk Testimony</u>.

274. LabMD's data security expert Adam Fisk ("Fisk") defines the Relevant Time as January 2005 through July 2010. (RX 533 (Fisk, Rep. at 3)).

275. Fisk has "13 years of professional experience building peer-to-peer applications with a focus on computer networking and security." (RX 533 (Fisk, Rep. at 4)).

276. Fisk received his "BA degree in Computer Science and US History from Brown University." (RX 533 (Fisk, Rep. at 4)).

277. "After graduating from Brown, [Fisk] moved to New York, NY to join LimeWire LLC in June of 2000 several weeks after its creation." (RX 533 (Fisk, Rep. at 4)).

278. Fisk is "the former Lead Engineer at LimeWire LLC, the creators of the LimeWire file sharing application, and an expert in peer-to-peer software, computer networking, and data security." (RX 533 (Fisk, Rep. at 3)).

279. Fisk testified LabMD took reasonable steps to secure PHI. (RX 533 (Fisk, Rep. at 32)).

280. LabMD's network adhered to best practices, not merely reasonable ones: It had

PUBLIC

two layers of properly configured firewalls protecting the network; there were proper user profiles on employee computers limiting the ability of non-managers to download files from the internet and to install applications. (RX 533 (Fisk, Rep. at 33)).

281. The Cisco 1841 Integrated Services Router deployed at LabMD had both firewall and intrusion prevention capabilities and exceeded the FTC's best practices recommendation. (RX 533 (Fisk, Rep. at 20, 33)).

282. The ZyWall5 IPSec firewall was a redundant layer of protection that shielded the LabMD network from unauthorized intrusion. (RX 533 (Fisk, Rep. at 33)).

283. LabMD did not deploy File Integrity Monitoring; however, LabMD had a policy against employees installing applications not necessary for the performance of their jobs and performed regular checks on employee machines in an effort to ensure that employees adhered to that policy. (RX 533 (Fisk, Rep. at 33)).

284. The best practices guidelines during the Relevant Period did not include File Integrity Monitoring in their recommendations. (RX 533 (Fisk, Rep. at 33)).

285. The 1718 File was not downloaded from LabMD through the firewall or due to any misconfiguration of LabMD's firewall. (RX 533 (Fisk, Rep. at 33)).

286. LabMD's firewall was properly configured and performed just as it should have by blocking incoming connections. (RX 533 (Fisk, Rep. at 33)).

286. Computers running LimeWire do not receive connection requests through the firewall because they are making outgoing connection requests to the Gnutella network. (RX 533 (Fisk, Rep. at 27)).

287. Due to a limited understanding of how LimeWire works, Dr. Hill erroneously

PUBLIC

concluded that LimeWire was running as an application accepting incoming connection requests through the firewall. (RX 533 (Fisk, Rep. at 26-27); (CX 0740 (Hill, Rep. at 43)).

288. Consequently, relying solely on the testimony of Kaloustian, Dr. Hill erroneously concluded that the 1718 File was accessed because LabMD's firewall was either disabled or misconfigured. (CX 0740 (Hill, Rep. at 36, 45)).

F. The "Day Sheets."

289. The Day Sheets were found while a search warrant was being served in Sacramento, California on October 5, 2012. (CX 0720 (Jestes, Dep. at 17-24)).

290. Complaint Counsel has not proven how the Day Sheets escaped LabMD's possession or how they ended up in California. (Hill, Tr. 220-221); (CX 0720 (Jestes, Dep. at 46)).

291. The Day Sheets were found in paper form, not electronic form in Sacramento. (CX 0720 (Jestes, Dep. at 58)).

292. Commission Staff was informed about the Day Sheets one week after the October 5, 2012 raid on the house in Sacramento. (CX 0720 (Jestes, Dep. at 61)).

293. The documents were transmitted to Commission staff in December 2012. (CX 0720 (Jestes, Dep. at 61-62)).

294. The Sacramento Police contacted FTC rather than LabMD because a Google search revealed the investigation arising from FTC's relationship with Tiversa and the 1718 File. (CX 0720 (Jestes, Dep. at 56)).

295. Complaint Counsel has not proven that any of the persons named on the Day Sheets were victims of identity theft. (CX 0720 (Jestes, Dep. at 57)).

296. LabMD was aware of its obligations under HIPAA to notify the patients listed on

PUBLIC

the Day Sheets and sent a letter notifying those individuals. (Daugherty, Tr. 1020-1021); (RX 348 (LabMD Patient Notification Letter [redacted])).

297. Hill concluded that LabMD's physical security was adequate. (Hill, Tr. 293).

G. LabMD Is Regulated Under HIPAA/HITECH.

298. At all times relevant, LabMD's PHI data-security practices were regulated by the U.S. Department of Health and Human Services ('HHS') under the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'), 45 U.S.C. § 1320d *et seq*. (U.S. Dep't of Health & Human Servs. (Health Information Technology), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/ (last accessed Aug. 9, 2015); (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5-7 ¶¶ 16-20, 31, 42-43, 48, 72)).

299. Neither HHS nor FTC has accused LabMD of violating HIPAA or HITECH. (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5-7 ¶¶ 16-20, 31, 42-43, 48, 72)).

300. "The FTC's Complaint in [this] Enforcement Action makes clear that LabMD was a 'health care provider' and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 12 ¶ 42)).

301. "The FTC [has not alleged or proved] that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 13 ¶43)).

302. 123. "The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 14 ¶ 48)).

303. "***In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.***" (CX0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 15 ¶ 52)) (emphasis added).

H. <u>The Commission Lacks Standards For Medical Companies</u>.

304. Daniel Kaufman, FTC's Rule 3.33 designee and Deputy Direct of the Bureau of Consmuer Protection, was ordered to testify regarding the following topics:

- The 1718 file, including the BOCP's relationship with Tiversa, Dartmouth College, and Eric Johnson.
- All data-security standards that have been used by the BOCP to enforce the law under Section 5 of the Federal Trade Commission Act since 2005.
- Consumers that have been harmed by LabMD's allegedly inadequate security practices.
- Relationship with the Sacramento Police Department relating to documents it found at a Sacramento "flop house" belonging to LabMD.

(Respondent's Deposition Notice of the Bureau of Consumer Protection, *In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Jan. 30, 2014) (on file with FTC Complaint Counsel and LabMD Counsel); (Letter from Complaint Counsel Laura Riposo Van Druff, FTC Complaint Counsel, to William A. Sherman, II, LabMD Counsel, regarding Daniel Kaufman's

PUBLIC

Rule 3.33 testimony) (Mar. 26, 2014) (on file with FTC Complaint Counsel and LabMD Counsel)).

305. As of the date of the taking of Kaufman's deposition the Commission had not produced information specifically focused on HIPAA Covered Entities, including LabMD, that advised them what was expected, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 176-177)).

306. As of the date of the taking of Kaufman's deposition, the Commission had not conducted any outreach specifically focused on HIPAA Covered Entities to advise them what the Commission expected from them, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 217)).

307. As of the date of the taking of Kaufman's deposition, the Commission had not promulgated any regulations or issued any formal guidance that would inform the general business public what it expected from such Covered Entities, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 215)).

308. Kaufman testified that the general business public must visit the FTC web site, review the FTC's complaints, orders, business education materials, attend FTC seminars and speeches, follow the FTC blog, follow FTC testimony before Congress, review FTC settlements, review FTC complaints, review FTC orders, review FTC press releases about data security cases, look at SANS, NIST and look at software and hardware product literature to determine what Section 5 requires in each given case. (RX 525 (Kaufman, Dep. at 190; 207-210); (Initial Pretrial Conference, *In the Matter of LabMD, Inc., a* corporation, FTC No. 9357, at 9-10) (Sept. 25, 2013)) (JUDGE CHAPPELL: "Have you -- in that regard, has the Commission issued guidelines for companies to utilize to protect this information or is there something out there for

PUBLIC

a company to look to?" MR. SHEER: "There is nothing out there for a company to look to. … JUDGE CHAPPELL: "Is there a rulemaking going on at this time or are there rules that have been issued in this area?" MR. SHEER: "There are no -- there is no rulemaking, and no rules have been issued …"); (RX 532 (Kaufman, Dep. at 163-220).

309. The thousands of pages of materials Complaint Counsel produced to LabMD in response to a request for information regarding standards consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief) (N.D. Ga.), at 16-17 ¶ 57)).

310. Some of these materials are of very recent vintage and dated after the events described in FTC's August 2013 administrative complaint allegedly occurred. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief) (N.D. Ga.), at 16-17 ¶ 57)).

311. Some of these materials are dated after August 28, 2013, when FTC issued this complaint. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 16-17 ¶ 57)).

312. The only regulations that FTC enforcement staff produced to LabMD did not

PUBLIC

apply to LabMD and implemented statutes that also did not apply to LabMD. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 16-17 ¶ 57)).

I. <u>Dr. Hill</u>.

313. In May, 2013, the Commission contacted Dr. Hill and asked her to assess LabMD's security program. She agreed to provide services to the FTC at that time. (RX 524 (Hill, Dep. at 55-56)).

314. Dr. Hill admits that portions of her report follow closely along with the allegations contained in paragraph 10 of the Complaint. (RX 524 (Hill, Dep. at 58)).

315. Hill relied upon the following materials in formulating an opinion in her report: (1) transcripts and exhibits from the FTC's investigational hearings and depositions of LabMD, its current and former employees, and third parties; (2) documents and correspondence provided to Complaint Counsel by LabMD and third parties in connection with the FTC's pre-Complaint investigation or this litigation; (3) industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners. (RX 524 (Hill, Dep. at 59-60)).

316. Hill states that Google is the place where an individual without her education, background, and experience could go to determine the industry and government standards and guidelines, as well as vulnerability databases, which establish best practices for the information security practitioner. (RX 524 (Hill, Dep. at 91-92)).

317. Other than the HIPAA Security Rule, Hill did not review any other portions of HIPAA in formulating her expert opinion. (RX 524 (Hill, Dep. at 65-66)).

PUBLIC

318. Dr. Hill did not (a) testify to knowledge of HIPAA data security regulations; (b) compare LabMD's PHI data security acts and practices with that of other healthcare providers of LabMD's size and nature; (c) consider LabMD's size notwithstanding HIPAA's emphasis on scalability. (Hill, Tr. at 296) ("For both—for small organizations and for large organizations, the guidelines are consistent"); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007); U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. Pts. 160, 162, & 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015); did not consult any medical industry data-security practices; did not apply the Commission's "reasonable" test but rather a more stringent "best practices" test; (d) identify best practices for each of the years during the relevant time (2005-2010), instead using 2014 standards and looking back (RX533 (Fisk, Rep. at 31-32); (e) profess knowledge of or apply medical industry standards; or (f) *"consider the FTC standards and guidelines"* in formulating her opinion whether LabMD's data security was reasonable.). (Hill, Tr. 230-231, 240-241) (emphasis added)).

319. Dr. Hill testified that "there's no such thing as perfect security, especially whenever there are humans involved in the configuration of the software." (Hill, Tr. 100).

320. At her deposition on April 18, 2014, Hill testified she referred exclusively to the HIPAA Security Rule in her report. (RX524 (Hill, Dep. at 64-65)).

321. At trial, Hill testified that she considered both the HIPAA Security Rule and HIPAA's six basic rules for assessment. (Hill, Tr. 231-232).

PUBLIC

322. Dr. Hill does not know whether HIPAA "governs the storage and transfer of health-related information by medical care providers." (Hill, Tr. 231).

323. Hill did not consider the HIPAA Security Rule or HIPAA in deciding whether or not LabMD was a HIPAA-covered entity. (Hill, Tr. 231) (Q. "So you're not intimately familiar with HIPAA then." A. "No, sir." Q. "Okay. And you did not consider HIPAA or HIPAA's guidelines in the formulation of your opinion in this case; correct?" A. "I considered the HIPAA security rule portion." Q. "And that's all with regard to HIPAA?" A. "Yes." Q. "And so it didn't play into your consideration or your opinion as to whether or not LabMD was a HIPAA-covered entity." A. "No. I didn't take that into consideration.").

324. Hill agrees LabMD received, maintained, utilized and stored health information. (RX 524 (Hill, Dep. at 65)).

325. Hill was not instructed by the FTC to give an opinion regarding HIPAA in the case against LabMD. (RX 524 (Hill, Dep. at 66)).

326. Hill admits that LabMD's physical data security was adequate. (RX 524 (Hill, Dep. at 118-119)).

327. Dr. Hill's report states: "For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information." (Hill, Tr. 216-219); (CX 0740 (Hill, Rep. at 20 ¶ 49)).

328. Dr. Hill was not asked by the FTC to assume that the type of harm set forth at page 20, ¶ 49 of her report actually had occurred. (Hill, Tr. 217); (CX 0740 (Hill, Rep. at 20 ¶49)).

329. Dr. Hill has no opinion with regard to the likelihood of harm because it was assumed in her report. (Hill, Tr. 218); (CX 0740 (Hill, Rep. at 20 ¶49)).

PUBLIC

330. Dr. Hill relies on CX0019 and the claim of Robert Boback and Tiversa that the 1718 File was found in four (4) places. (CX 0740 (Hill, Rep. at 17 ¶ 46)) ("A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B."); (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found)); (CX 0740 (Hill, Rep. at 19, 59, 61)).

331. Dr. Hill did not consider HIPAA's definition of protected health information in formulating her opinion about LabMD data security practices. (RX 524 (Hill, Dep. at 71)).

332. Hill did not consider the fact that LabMD was a covered entity as defined by HIPAA. (RX 524 (Hill, Dep. at 71)).

333. Hill did not rely on the data security standards published by the FTC. (Hill, Tr. 230-231); (RX 524 (Hill, Dep. at 71-72)).

334. HIPAA is based on risk assessment and scalability, which Hill's reports and opinions fail to properly consider. (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3 ("Factors that determine what is 'reasonable' and 'appropriate' ***include cost, size, technical infrastructure and resources.***") (emphasis added), 12 ("***The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances.*** Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L.

No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)).

332. "The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity." (HHS: The Security Rule, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html) (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)).

333. "The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." (HHS: The Security Rule, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html) (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007)).

333. HHS does not require what Dr. Hill does with respect to data encryption and integrity monitoring and are more prescriptive than HIPAA or inconsistent with HHS guidance, including encryption at rest (an addressable requirement of 45 C.F.R. § 164.312(a)(1)), encryption in transit (an addressable requirement of 45 C.F.R. § 164.312(e)(1)), and file integrity monitoring (not addressed specifically by the Security Rule). (CX 0740 (Hill, Rep. at

PUBLIC

20 ¶ 55, 22-23 ¶ 61(b)(bullet 2), 24-25 ¶ 65, 26-28 ¶ 68(c), ¶ 69)); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007), 12)) ("***Covered entities use open networks such as the Internet and e-mail systems differently***. ***Currently no single interoperable encryption solution for communicating over open networks exists***. ***Adopting a single industry-wide encryption standard in the Security Rule would likely have placed too high a financial and technical burden on many covered entities. The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use. A covered entity should discuss reasonable and appropriate security measures for the encryption of EPHI during transmission over electronic communications networks with its IT professionals, vendors, business associates, and trading partners.***") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last accessed Aug. 9, 2015); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007), at 15-17) (Security Standards Matrix (Appendix A of the Security Rule)), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last accessed Aug. 9, 2015)).

334. Dr. Hill's opinion on risk assessment based upon NIST Security Series Reference 800-30 conflicts with HIPAA guidance and regulations. (CX 0740 (Hill, Rep. at 29-30 ¶ 74); (Dep't of Health & Human Servs. (HIPAA Security Series (**6 Basics of Risk Analysis and Risk Management**) (Volume 2/ Paper 6) (6/2005: rev. 3/2007), 3)) ("…**only federal agencies are required to follow federal guidelines like the NIST 800 series** … ***Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that***

PUBLIC

organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.") (italic emphasis in original) (bold emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf (last accessed Aug. 9, 2015).

335. Dr. Hill has never given an opinion regarding the adequacy of a company's operating on a day-to-day basis and has no medical industry experience. (RX 524 (Hill, Dep. at 73)).

336. In rendering her opinion, Dr. Hill has never conducted an on-site visit to a business to review its existing data security as it operates on a day-to-day basis. (RX 524 (Hill, Dep. at 73)).

337. In rendering her opinion, Dr. Hill has never conducted an on-site visit to a business (including LabMD, in this case) to review and evaluate its existing data security polices, practices, and procedures. (RX 524 (Hill, Dep. at 73)).

338. Dr. Hill formulated the definition of "comprehensive information security program" in her report based solely on her personal experience. (RX 524 (Hill, Dep. at 73-74) (Ex. 1 at p. 19 ¶ 52) (as Dep. Ex. RX-1)).

339. The primary information Dr. Hill used for reaching the conclusions in her report regarding LabMD's data security was her background and experience. (RX 524 (Hill, Dep. at 86)).

340. Hill did not rely on FTC's "five key principles" to data security listed in the "Protecting Personal Information: A Guide for Business" issued November 2011 – the "five key

PUBLIC

principles" do not match Dr. Hills "seven factor test" and do not include "defense in depth," which Dr. Hill testified LabMD was supposed to have discovered in 2009. (Hill, Tr. 235-236); (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)).

341. The Commission has never published data security standards or guidance for medical service providers regulated by HIPAA or, prior to this case, suggested Section 5 might prohibit what HIPAA permits. (RX 526 (Complaint Counsel's Amended Response to LabMD's Requests For Admission No. 1, at 4 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9257) (Apr. 1, 2014)).

342. Between 2005 and 2010, the FTC did not prescribe any rules or promulgated regulations regarding data-security, data security practices or data security standards for PHI that defines what acts are prohibited or required under Section 5 of the FTC Act, 15 U.S.C. § 45, as related to PHI. (RX 526 (Complaint Counsel's Amended Response to LabMD's Requests For Admission No. 1, at 4-5 (In the Matter of LabMD, Inc., a corporation, FTC No. 9257) (Apr. 1, 2014)).

343. FTC's Deputy Director of BCP and designated Rule 3.33 witness, Daniel Kaufman admitted that the FTC lacks any Section 5 "unfairness" data security standards and that the FTC has not promulgated data security regulations. (RX525 (Kaufman, Dep. at 211, 215)) (Q. "So does the term "data security" appear in Section 5 of the Act?" A. "No, it does not.") (Q. "It's correct that the FTC has not promulgated regulations with regard to data security for personal identifying information?" A. "In connection with Section 5 of the FTC Act, that is correct. We have, nevertheless, consistently applied Section 5 and the unfairness test to assess

PUBLIC

the reasonableness of the security practices." Q. "But that's not promulgation of regulation; is that correct?" A. "Yes.").

344. Dr. Hill's testimony is inconsistent in stating that she "was not asked to make any assumptions about the inadequacies of LabMD's data security" while also assuming that the 1718 File was taken from LabMD's possession as a result of inadequate data security. (Hill, Tr. 219-220) (Q. "Were you asked to assume that the 1718 File escaped the possession of LabMD due to some inadequacy in LabMD's data security?" A. "I was not asked to make any assumptions about the inadequacies of LabMD's data security.").

345. Dr. Hill states "[t]here's no definitive evidence of how [the 1718 File] left LabMD's possession" as a result of the downloading of an unauthorized program onto a workstation at LabMD. (Hill, Tr. 220).

346. Dr. Hill did not have access to the Wallace testimony. (Wallace, Tr. 1337); (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Tr. 80-325) (Hill testimony) (May 20, 2014)).

347. Dr. Hill has no opinion about exactly how the 1718 File was taken from LabMD. (Hill, Tr. 219).

348. Dr. Hill failed to address scalability as required by HIPAA. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007); (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3, ("***Factors that***

PUBLIC

determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources.") (emphasis added), 12 ("***The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.***") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164)).

349. The 1996 HIPAA statute states that in promulgating information security regulations, the Secretary must take into account the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary), and the preamble to the HIPAA Security Rule (p. 8335) states accordingly that one of the foundations of the rule is that it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes. (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

350. Based upon public comments received during the rulemaking process for HIPAA's Security Rule, HHS crafted a unique information security regulatory scheme that separated 'implementation specifications – the types of very specific security requirements emphasized by the FTC's expert – into two classes: "required" and "addressable." (60 Fed. Reg. 8336 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

PUBLIC

351. HHS stayed consistent with the original information security regulatory separated, "two–class" theme in its most recent updates to the HIPAA Privacy and Security rules in 2013. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162,164); (U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last visited Aug. 9, 2015)).

352. HHS utilized a scalable model in promulgating HIPAA's Privacy and Security Rules, such that these Rules reflect HHS's challenge in complying with Congressional intent in establishing a security rule to address reasonable and appropriate security requirements for the range of organizations in healthcare that differ greatly in operations, size, complexity, and resources. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162,164); (U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last visited Aug. 9, 2015)).

353. HIPAA demands that a covered entity perform a risk assessment in good faith and take actions to secure Electronic Protected Health Information ("EPHI") based on the findings of that risk assessment. (74 Fed. Reg. 42740, 42760 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 164, §164.402(2)(i-iv); (U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, at 71, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013)), *available at*

PUBLIC

http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015)).

354. In assessing HIPAA noncompliance, it is necessary to determine if a risk assessment was performed in good faith, and resulted in a process that included implementation of requirements and appropriate responses to "addressable" issues. (74 Fed. Reg. 42740, 42760 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 164, §164.402(2)(i-iv); (U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, at 71, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015)).

355. Given the limited knowledge of information technology by many small health care providers, especially during the early years of HIPAA Security, many of the security measures they were advised to adopt by HHS issued guidance related to physical and administrative security rather than specific technical security. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164)).

356. The preamble to HIPAA's Security Rule provides "that encryption should not be a mandatory requirement for transmission over dial-up lines. . . . [and] when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. . . . [so] the use of encryption in the transmission process [is] an addressable implementation specification." (60 Fed. Reg. 8335, 8357 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164) (corresponding to 45 C.F.R. §164.312(e)(1) of the Rule on Transmission Security)).

PUBLIC

357. After almost ten years of complying with HIPAA security rules, the guidance has not changed substantively regarding implementing security for small providers in the healthcare industry, based upon HHS's understanding of the realities associated with implementing security for small providers in the healthcare industry. (U.S. Dep't of Health & Human Servs., Office of the Nat'l Coordinator for Health Info. Tech., Guide to Privacy & Security of Electronic Health Info., 13-14 (Version 2.0) (Apr. 2015), *available at* http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf (last accessed Aug. 9, 2015)).

355. Dr. Hill's opinion did not reference or rely on the relevant HIPAA statutes, regulations and guidance. (RX 524 (Hill. Dep.) (Apr. 18, 2014)); (CX 0740 (Hill Rep.) (Mar. 18, 2014)); (Hill, Tr. 80-325); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

356. Dr. Hill did not properly apply the accordance with the HIPAA Security Rule, and did not take account, as required by the 1996 HIPAA statute, the needs and capabilities of small health care providers such as LabMD. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)).

357. Dr. Hill opined that between January 2005 and July 2010 "LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures." (CX 0740 (Hill, Rep. at 20)).

358. Her opinion does not specify precisely how LabMD failed at any given point in

PUBLIC

time. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

359. Hill further opined that "LabMD did not develop, implement or maintain a comprehensive information security program to protect consumer's Personal Information." (CX 0740 (Hill, Rep. at 24)).

360. According to Dr. Hill, maintaining a comprehensive information security program includes employing a defense in depth strategy, which in turn includes addressing the seven principles she outlines in her report. (Hill, Tr. 307-309).

361. The seven principles are: (1) Don't keep what you don't need, (2) Patch, (3) Ports, (4) Policies, (5) Protect, (6) Probe, and (7) Physical. (CX 0740 (Hill, Rep. at 13-15)).

362. Dr. Hill is unaware of any document that cites there are "seven principles for a comprehensive information security program." (Hill, Tr. 242-243).

363. Dr. Hill opines on data security standards relating to the general Information Technology industry. (CX 0740 (Hill, Rep. at 1-46); (Hill, Tr. 234); (RX 524 (Hill, Dep. at 61)).

364. Dr. Hill admits that she has never worked for a medical provider or lab. (RX 524 (Hill, Dep. at 150)).

365. Dr. Hill only became aware of the defense in depth strategy circa mid-2009. (Hill, Tr. 306).

366. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that penetration testing was never done. CX 0740 (Hill, Rep. at 38); (Hill Tr. 276)).

PUBLIC

367. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that firewalls were disabled on servers that contained personal information. (CX 0740 (Hill, Rep. at 38); (Hill, Tr. 274-275).

368. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that personal information was transmitted and stored in an encrypted format. (CX 0740 (Hill, Rep. at 38)).

369. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft. (CX 0740 (Hill, Rep. at 42)).

370. Dr. Hill relies only on factual information from Curt Kaloustian's Investigational Hearing Transcript to conclude that LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network. (CX 0740 (Hill, Rep. at 47)).

371. Kaloustian was compelled to give testimony pursuant to a FTC Civil Investigative Demand. (CX 0750 (CID to Curt Kaloustian)).

372. The nonpublic proceeding took place on May 3, 2013 before FTC attorneys Laura Riposo Van Druff and Alain Sheer. (CX 0735 (Curt Kaloustian, IHT (with attached Errata), at 1-7)).

373. Prior to this hearing, on March 20, 2013, Commission staff was notified by LabMD's counsel that contacting former employees of LabMD was improper without first informing the company's legal counsel so as to properly preserve the attorney-client privilege and that Kaloustian was subject to a confidentiality agreement. (CX 0735 (Curt Kaloustian, IHT (with attached Errata), at 1-7)).

PUBLIC

374. LabMD was never told Kaloustian was to be deposed by FTC. (CX 0735 (Curt Kaloustian, IHT (with attached Errata) at 1-7)).

375. LabMD did not have counsel present and could not assert the attorney-client privilege. (CX 0735 (Curt Kaloustian, IHT (with attached Errata) at 1-310)).

376. At the time he testified to FTC on May 3, 2013, Kaloustian had been terminated by LabMD for inadequate work performance. (RX 415 (Kaloustian background check/A. Simmons' resignation, at 1)) ("Terminated for failure to perform job duties").

377. Dr. Hill only relies on information from Robert Boback and Tiversa to conclude that "[c]opies of the 1718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom." (CX 0740 (Hill, Rep. at 17)).

378. Dr. Hill admits that in rendering her expert opinion that LabMD's data security was insufficient, that she does not cite to any purported FTC standards and guidelines. (Hill, Tr. 230-23, 240-241).

379. Dr. Hill was not asked and did not opine regarding LabMD's current data security practices or whether those practices now cause substantial consumer injury and are unreasonable. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

380. Dr. Hill was not asked and did not opine whether the allegedly unreasonable LabMD's data security practices during the 2005-2010 time-frame are "likely" or probable to reoccur, and if so, to cause harm in the future. (ALJ Chappell, Tr. 513-514) ("The rule is, a witness who's an expert is limited to opinions contained in the expert report that is vetted properly through discovery. . . ."); (Hill, Tr. 218) ("Q. So it's fair to say then that you have no opinion with regard to the likelihood of harm because it was assumed in your report; correct? A. I have no opinion, yes.").

PUBLIC

381. To the extent Dr. Hill did opine regarding the likelihood of harm, that opinion was based on perjured and fraudulent evidence provided by Boback and Tiversa. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

382. Although Dr. Hill considered LabMD's data security for the time period of 2005-2010, she used and evaluated sources published *after* 2010. (CX0740 (Hill, Rep. at 4-8)).

383. Dr. Hill did not consider FTC's standards and guidelines in formulating her opinion. (Hill, Tr. 230-31, 240-41).

384. Complaint Counsel did not ask Dr. Hill to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

385. Complaint Counsel did not ask Dr. Hill to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

J. <u>Rick Kam</u>.

386. Complaint Counsel hired Rick Kam to provide an opinion regarding the "risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information." (CX 0742 (Kam, Rep. at 5)).

387. FTC paid Kam "$350 per hour" for his opinions and testimony against LabMD. (CX 0742 (Kam, Rep. at 5); (LabMD's Mtn. *In Limine* to Exclude Kam's Testimony, at 1 (*In the Matter of LabMD, Inc., a corporation*, FTC Dkt. No. 9357, FTC Doc. No. 264) (Apr. 22, 2014))

[redacted] (RX 522 (Kam, Dep. at 181); Kam is not qualified to testify as an expert on the risk of harm to consumers because he [redacted] (LabMD's Mtn. In Limine to Exclude Kam's Testimony (*In the Matter of LabMD, Inc., a corporation,* FTC No. 9357, at 8 (Apr. 22, 2014); (RX 522 (Kam, Dep. at 181-182)).

388. Kam's only educational degree is in management and marketing. (Kam, Tr. 516).

389. Kam has no expertise in computer data security or computer network security. (Kam, Tr. 518).

390. Kam's personally-developed methodology is not generally accepted in the fields of medical or data privacy or statistical analysis, nor has any work based upon such methodology been peer-reviewed or published. (CX 0742 (Kam, Rep. at 17-18); (RX 522 (Kam, Dep. at 46)).

391. In developing his personal four–factor methodology, Kam never used statistical analysis, never spoke to data privacy professionals, and never allowed any review of his methodology because of confidentiality agreements in place. (Kam, Tr. 549-552) (Q. "All of your work with your clients is subject to confidentiality agreements; right?" A. "Yes." . . . Q. "Well, did you consult statistical analysis to develop your four factors?" A. "I don't believe I used statistical analysis to develop that." . . . Q. "Did you discuss with these other privacy professionals how many factors to include in the test?" A. "You know, I don't recall asking – thinking about it in that context. No.").

392. Kam's personally-developed methodology has never been published, peer reviewed, or reviewed in any form. (Kam, Tr. 552).

393. All of Kam's work has been under the patronage of client-consulting arrangements governed by confidentiality agreements. (RX 522 (Kam, Dep. at 48-49) [redacted] (LabMD's Mtn. *In Limine* to Exclude Kam's Testimony, at 4 (FTC Doc. No. 264) (Apr. 22, 2014)).

394. Kam's methodology, report, and opinions they cannot be tested or publicly reviewed due to governing confidentiality agreements and the fact that such methodology was developed by Kam in consultation with hiring counsel. (Kam, Tr. 551-552); (RX 522 (Kam, Dep. at 46)) (Q. [redacted]

395. Complaint Counsel provided Kam with the "Transcript of the deposition of Robert Boback, CEO of Tiversa, dated November 21, 2013, with supporting exhibits," including CX0019, upon which Kam based his report, opinions, and testimony. (CX 0742 (Kam. Rep. at 6)).

396. Kam is the "president and co-founder of ID Experts . . . based in Portland, Oregon." (CX 0742 (Kam, Rep. at 3)).

397. Lawrence Ponemon sat on the board of advisors for Kam's company for six (6) to nine (9) months in 2013. (RX 522 (Kam, Dep. at 172-174).

PUBLIC

398. Kam knows Lawrence Ponemon is on the board of advisors for Tiversa. (Kam, Tr. 552-553).

399. Kam used and relied upon the 2013 Ponemon Survey in his report, opinions, and testimony. (Kam, Tr. 484-486); [redacted]

401. Kam's company ID Experts paid $50,000 to the Ponemon Institute for a 2014 data privacy and security report. (Kam, Tr. 554).

402. Kam agreed with the following conclusion regarding medical identity theft contained in the 2013 Ponemon survey: [redacted]

403. The response rate to the 2013 Ponemon Survey was 1.8 %. (Kam, Tr. 540).

404. Kam did not conduct a regression analysis for the 2013 Ponemon Survey because he is not a statistician and does not know the definition of a regression analysis. (Kam, Tr. 540) (Q. "Mr. Kam, do you know what a regression analysis is?" A. "I'm not a statistician. I wouldn't be able to give you an accurate definition." Q. "So then you didn't conduct a regression analysis on the Ponemon survey, did you?" A. "No.").

405. The 2013 Ponemon Survey had a non-response bias. (Kam, Tr. 540) (Q. "Do you know what a nonresponse bias is?" A. "I believe so." Q. "What is it?" A. "It's if people who

PUBLIC

were not -- who were surveyed did not respond might have a different answer to the question." Q. "Under your understanding of a nonresponse bias, the Ponemon survey has a nonresponse bias, doesn't it?" A. "Yes, it does.").

406. The 2013 Ponemon Survey is unreliable because it collected results using a Web-based collection method, and compensated respondents. (Kam, Tr. 541) (Q. "The Ponemon survey collected its results using a Web-based collection method, didn't it?" A. "I believe that to be the case. Yes." Q. "The Ponemon survey compensated respondents, didn't it?" A. "They did, yes.").

407. The 2013 Ponemon Survey has a sampling frame bias. (Kam, Tr. 541) (Q. "Do you know what a sampling frame bias is?" A. "I believe it has something to do with the sample and who was actually -- who actually took the survey." Q. "The Ponemon survey has a sampling frame bias, doesn't it?" A. "It does. . . .").

408. Kam relied upon Robert Boback's November 2013 testimony when analyzing the risk of harm under the first three (3) factors of his four-factor test. (Kam, Tr. 542).

409. Kam assumed as true Robert Boback's November 2013 testimony that law enforcement had apprehended someone suspected of identity theft or fraud using one of the addresses where the 1718 File was found. (Kam, Tr. 542).

410. Kam relied upon Robert Boback's November 2013 testimony and multiple levels of hearsay and supposition regarding IP address 173.16.83.112. (Kam, Tr. 544-545) (Q. "On page 64 line 17, Mr. Boback says, of one of the IP addresses, 'I believe that the 173.16.83.112 had law enforcement, federal law enforcement after that individual for identity theft or fraud of some sort. Tiversa wasn't involved in that, though. QUESTION: 'How do you know this?' ANSWER: 'We heard this through federal law enforcement, you know, surreptitiously through

PUBLIC

federal law enforcement. But we don't know specifically.' Did I read that correctly?" A. "Yes." Q. "Mr. Boback says 'I believe' instead of 'I know.' . . ." Q. "Mr. Boback says 'I believe' instead of 'I know,' doesn't he?" A. "He does say that in his testimony." Q. "He uses the word 'surreptitiously'?" A. "Yes." Q. "He says he doesn't know specifically about the incident." A. "I agree.").

411. Kam used unreliable, double hearsay evidence found at pages 64-65 of Robert Boback's November 2013 deposition as the factual underpinning for Kam's assessment of the risk of harm in this case. (Kam, Tr. 545-546) (Q. "When asked, on page 64, 'Do you know what action was taken?' Mr. Boback answered, on page 65, 'I had heard that the individual at 173.16.83.112 was either detained or arrested in an Arizona Best Buy buying multiple computers. I don't know the outcome of this case. I'm not privileged to any of that information.' Did I read that correctly?" A. "You did." Q. "Mr. Boback says he heard the individual was detained or arrested instead of he knew; isn't that right?" A. "Yes." Q. "He doesn't say who he heard it from?" A. "No." Q. "He does not say who was arrested?" A. "No. . . ." Q. "He says he doesn't know the outcome of the case pertaining to identity theft in Arizona; right?" A. "Yes." Q. "And you used this information as the factual underpinning for your assessment of the risk of harm; right?" A. "For some of it, yes.").

412. Kam relied upon the CLEAR spreadsheet. (CX 0742 (Kam, Rep. at 7, 23); (Tr. 371-373)).

413. The CLEAR spreadsheet was excluded from evidence. (ALJ Chappell, Tr. 371-373)) (JUDGE CHAPPELL: ". . . to the extent you want to use this document against respondents, and if I understood what you said, to show that these Social Security numbers were used and that might for some later witness be used to say that's indicative of a possible identity

PUBLIC

theft, ***we don't know if the Social Security number on the day sheet was correct.*** We don't know if the Social Security number that the CLEAR data reflected was accurate. . . .") (emphasis added)).

414. Kam cannot identify a single actual victim of identity theft caused by LabMD's acts or practices. (Kam, Tr. 507).

415. For the relevant time period 2007-2010, Kam cannot identify a single actual victim of identity theft or fraud among the names on the LabMD Day Sheets. (Kam, Tr. 507) (Q. ". . . [D]o you know of any actual victims of identity theft or fraud . . . among the names that were on the LabMD day sheets in 2007?" A. "No." Q. "In 2008?" A. "No." Q. "In 2009?" A. "No." Q. "In 2010?" A. "No.").

416. Complaint Counsel instructed Kam to assume LabMD's data security practices were unreasonable for the Relevant Time. (Kam, Tr. 517-518) (Q. "At the bottom of page 5, you wrote, 'For the purposes of my analysis, I have assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks.' Did I read that correctly?" A. "You did." Q. "So in your expert opinion, in providing your expert opinion, you're not analyzing any of LabMD's specific practices with respect to its computer networks; correct?" A. "Correct.); (Kam, Tr. 518) (Q. "You don't know the degree to which LabMD's data security practices were adequate or not, you just assumed they were inadequate; correct?" A. "That's correct.").

417. Kam testified at trial that his report would be "valid in full" even if LabMD had "executed exemplary levels of data security practices" at all times relevant to this case. (Kam, Tr. 521) (Q. "So, Mr. Kam, your testimony is that even if it were found that LabMD had

PUBLIC

executed exemplary levels of data security practices, your report would still be valid in full." A. "Given what I just said earlier, yes.").

418. Kam relied on Robert Boback's testimony to conclude that the 1718 File was found on four IP addresses, and was available as late as November 21, 2013 on the peer to peer network. (CX 0741 (Van Dyke, Rep. at 7)).

419. Kam assumed that the suspects in whose Sacramento house LabMD's Day Sheets were found had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012." (RX 522 (Kam, Dep. 147-148)).

420. Kam estimated that there would be 76 victims of medical identity theft due to the alleged disclosure of the 1718 File. (CX 0742 (Kam, Rep. at 19)).

421. Kam admitted that his expert opinion did not account for the absence of any evidence of victims in this case. (Kam, Tr. 532).

422. Kam repeatedly mentions the possibility of embarrassment, specifically from the alleged exposure of CPT codes, which indicate that a person has paid for a particular laboratory test to be run, as an element of damage. (CX 0742 (Kam, Rep. at 16, 21)).

423. Kam acknowledges that CPT codes indicate only that testing has been paid for, and do not "indicate a diagnosis." (CX 0742 (Kam, Rep. at 16)).

424. Complaint Counsel did not ask Kam to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. (CX 0742 (Kam Rep.); (RX 522 (Kam Dep.); (Kam, Tr. 377-573)).

425. Complaint Counsel did not ask Kam to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. Kam's testimony suggest bias as his

PUBLIC

method was simply to place the heaviest weight on whichever factor disfavored LabMD most. (CX 0742 (Kam Rep.); (RX 522 (Kam Dep.); (Kam, Tr. 377-573)).

426. Kam admitted that in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532).

427. Kam admitted that his expert opinion did not account for the absence of any evidence of victims in this case. (Kam, Tr. 532).

K. <u>Jim Van Dyke.</u>

428. Jim Van Dyke ("Van Dyke") was engaged by FTC to "assess the risk of injury to consumers whose personally identifiable information has been disclosed by LabMD, Inc. without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure." (CX 0741 (Van Dyke, Rep. at 2)).

429. Complaint Counsel did not ask Van Dyke to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. [redacted]

430. Complaint Counsel did not ask Van Dyke to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. [redacted]

431. Van Dyke assumed that "LabMD failed to provide reasonable and appropriate for the personally identifiable information maintained on its computer networks." (CX 0741 (Van Dyke, Rep. at 2)).

432. Van Dyke also assumed that the "1718 File and the day sheets were found outside of LabMD as a result of a data breach." (Van Dyke, Tr. 678-679).

PUBLIC

433. Van Dyke's opinion was "LabMD's failure to provide reasonable and appropriate security for [the 1718 File, Day Sheets, and personally identifiable information maintained on LabMD's computer network] places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of what is commonly called "identity theft . . ." (CX 0741 (Van Dyke, Rep. at 3)).

434. Van Dyke's opinions were based on pre-January 2010 practices only. (CX 0741 (Van Dyke, Rep. at 2, 4)).

435. Van Dyke admitted that he does not have extensive educational experience with information technology. (RX 523 (Van Dyke, Dep. at 11-13, 19)).

436. Van Dyke is not a statistician. (Van Dyke, Tr. 674) (Q. "[Mr. Van Dyke,] you're not a statistician; correct?" A. I'm not personally a statistician, no."); (Van Dyke, Tr. 718-719)) (JUDGE CHAPPELL: "And you, if I take it -- if I'm correct, do not have a statistical background; is that correct?" THE WITNESS: "I think it's most accurate to say I do have a statistical background. I do not have a dedicated educational degree in statistics, no, but I've worked in that field and taken dedicated courses in that subject." JUDGE CHAPPELL: "Would you call yourself a statistician?" THE WITNESS: "No, I would not, Your Honor.").

437. Complaint Counsel first contacted Van Dyke to serve as an expert in this case before the Knowledge Networks Survey was fielded in October 2013. (Van Dyke, Tr. 636) (Q. "And the survey was fielded by Knowledge Networks in October of 2013?" A. "Correct." Q. "Do you know how long from the time the survey was first fielded or sent to the panel that the survey was completed?" A. "To the best of my recollection, that fielding began on October 9, 2013 and concluded on October 23, 2013. . . ."); (Van Dyke, Tr. 638) (Q. ". . . When were you contacted by the FTC to – when did they ask if you would be willing to render an opinion in this

PUBLIC

case?" A. "Oh, I could not answer with precision on that. That was sometime in the first half of 2013." Q. "Okay. So it was prior to the survey being fielded; correct?" A. "That is correct.")).

438. Van Dyke admits that he never considered any of the specific facts of the case. (RX 523 (Van Dyke, Dep. at 72-73) (Q. "So your entire opinion is based on the responses to the survey that was conducted in October of 2013?" A. "Yes, for the purpose of this statement that's true, yes." Q. "So the actual facts of the LabMD case, outside of the presumption that the information was exposed to unauthorized third parties, really doesn't matter and really wasn't taken into consideration in your analysis when it comes to these percentages; correct?" A. "That's correct." Q. "And the actual facts of what actually happened in the case concerning LabMD do not play a factor in your conclusions and opinions as it relates to how much time a consumer will spend correcting what occurred as a result of the LabMD breach; correct? A. ". . . THE WITNESS: Yes, that is correct, yes.")).

439. Van Dyke did not contact any of the referring physicians' patients listed in the 1718 File. (CX 0741 (Van Dyke, Rep. at 1-21)).

440. Van Dyke's report and opinions rely on Boback's November 2013 testimony. (RX 523 (Van Dyke, Dep. at 107-108) (Q. . . . "You are saying that your findings in your report including the figures that appear in Figure 2 and Figure 3 of your report, are relevant and applicable to the incident that occurred in this case, the exposure of the information by LabMD, because Mr. Boback testified in November 2013 that the insurance aging report could be found in multiple locations?" A. "Yes, because the insurance aging report could be found in multiple locations." Q. "At the time that he testified?" A. "At the time that he testified.");
(RX 523 (Van Dyke, Dep. at 109-110) (Q. "How is time a factor in your calculations other than 12 months from the time that the survey respondents responded?" A. ". . . we chose the time

period because Mr. Boback testified that the time that he most recently saw evidence of all those SSNs out there, that are likely to lead to identity fraud in my opinion, that time period fell within our 12–month measurement period.”)).

441. Van Dyke’s report and opinions at trial regarding ongoing identity theft or medical identity theft specifically relied upon Boback’s November 2013 testimony regarding the 1718 File and the Day Sheets. (Van Dyke, Tr. 645-646) (Q. “Would it matter if the 1718 File and the day sheets were in the hands of governmental entities?” A. “If that was an authorized party, in other words, not a data breach, then that would matter because the calculations wouldn't apply here. But that was not the case in this instance.” Q. “How do you know it wasn’t the case in this instance?” A. “Because, according to the testimony that I’ve read, the 600 day sheets were found in the possession of individuals that have pleaded no contest to identity theft. And in reading through Mr. Boback’s testimony as of late 2013, the 9300 PII records were found in as many as four locations, four IP locations, so that’s what I’m relying on, is his statement.” Q. “Are you aware of who owned those IP locations where the 1718 File was found?” A. “No. I’m relying on his testimony.”); (Van Dyke, Tr. 667-660) (Q. “I still don’t understand how the 30.5 percent figure relates to those individuals whose names appear on the 1718 File when those individuals were never notified of a data breach. . . .” A. . . . “That relates to the 1718 File because we know that the 1718 File, from the testimony of Mr. Boback, that it was found in four places where it didn’t belong, so that’s the indicator of the first thing, exposure of the data. And I use that to make an estimate, a projection -- pardon me -- of the amount of harm that those people who have had their data exposed in an unauthorized way are likely to encounter.”)).

442. Van Dyke disregarded the facts underlying how the 1718 File was taken from LabMD. (RX 523 (Van Dyke, Dep. at 39) (Q. “Were you told that it was a fact in this case, were

PUBLIC

you told or did you see any information that you were provided that indicated that someone other than Tiversa had found the 1718 file outside of LabMD's possession?" A. "I don't believe so." Q. "In terms of your analysis does it matter how the insurance aging file was taken from LabMD?" A. "That's something I haven't considered in my opinion." Q. "In terms of your analysis would it matter how it was taken from LabMD?" A. "Again, I haven't give any consideration to that."); (Van Dyke, Tr. 645) (Q. ". . . In terms of arriving at your conclusions and your opinions, does it matter to you how the 1718 File and the day sheets escaped LabMD's possession?" A. "No, it does not matter to me.")).

443. Van Dyke's analysis failed to include any temporal component as regards the 1718 File, and assumed the same amount of damage would occur from the disclosure of the information regardless of whether it was available for two month or four years. (RX 523 (Van Dyke, Dep. at 41-42)) (Q. "So when the insurance aging file escaped the possession of LabMD did not figure into your considerations or analysis at all?" A. "No, not when it escaped." Q. "Does your analysis have a temporal component to it at all as it relates to the insurance aging file?" A. "No, it does not." Q. "So your analysis does not take into account the length of time that the information contained on the insurance aging file has been exposed to unauthorized third parties?" A. "No, it does not.").

444. Van Dyke's methodology and analysis as contained in his report and opinions is based on Javelin's 2013 ID Fraud Survey. (CX 0741 (Van Dyke, Rep. at 4); [redacted]

445. Javelin's 2013 Fraud ID Survey relied upon Knowledge Networks, which was a vendor paid by Javelin for the last four (4) years to provide access to survey respondents. (CX 0741 (Van Dyke, Rep. at 4 n.6); (RX 523 (Van Dyke, Dep. at 113-114)).

446. Van Dyke's report, opinions, and the 2013 Fraud ID Survey erroneously applied 2013 data to the facts of the 1718 File disclosure. (RX 523 (Van Dyke, Dep. at 96); (CX 0741 (Van Dyke, Rep. at 12 Fig. 3)).

447. The respondents' answer to Question 2 under Figure 1 of the Van Dyke report was confined to the 12-month period preceding the Survey, October 2013 back to October 2012. (Van Dyke, Tr. 655) (Q. "So we've got two time periods going on in that question; correct? One, been notified within the past twelve months; correct?" A. "Yes." Q. "And it's the past twelve months of responding to the survey." A. "That's correct." Q. "So the time period runs from the day the respondent responds to the survey twelve months back from that day; correct?" A. "That's right."); (CX 0741 (Van Dyke, Rep. at 8 Fig. 1)).

448. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the total one year fraud amount (in billions) for the years 2006 through and including 2012. [redacted]

449. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean fraud amount per fraud victim for the years 2006 through and including 2012. [redacted]

450. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the median fraud amount per fraud victim for the years 2006 through and including 2012. [redacted]

PUBLIC

451. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean consumer cost for the years 2006 through and including 2012. [redacted]

452. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean resolution time (hours) for the years 2006 through and including 2012. [redacted]

453. The information contained in Figure 3 of the 2013 Fraud ID Report contradict and/or belie Van Dyke's report and opinions as to whether and to what extent consumers were at significantly higher risk of becoming victims of identity fraud and/or medical identity theft/fraud for the relevant time period in this case which is January 2005 to July 2010. (CX0741 (Van Dyke, Rep. at 3)); [redacted]

454. Van Dyke's report, opinions, and trial testimony relied upon the 2013 Ponemon Survey on Medical Identity Theft which was financed by Richard Kam's Company, ID Experts. (CX 0741 (Van Dyke, Rep. at 18)).

455. Van Dyke could not identify a single victim of identity theft or fraud, medical theft or fraud, or any consumer injury as a result of the 1718 File or the Sacramento Day Sheets. (CX 0741 (Van Dyke, Rep. at 1-21)).

456. Van Dyke's projection is erroneous that within one (1) year of unauthorized disclosure, 7.1% of the individuals on the 1718 File list should have experienced non-card identity fraud because victims of identity theft from the 1718 File and the Day Sheets do not exist. (Van Dyke, Tr. 692-693)) (Q. "***So if the information contained on the 1718 File was exposed in February of 2008, then sometime between February of 2008 and February of 2009,***

PUBLIC

7.1 percent of those individuals should have experienced existing non-card fraud." A. "That would be my projection, yes." Q. "Okay. And if the evidence is that none of those individuals experienced existing non-card fraud during that period of time, is there -- I mean, how would you explain that or could you explain it?" A. "I actually couldn't give you a response to that because what I'm solely relying on is, you know, the ten years of surveying these populations. Now we're over 5,000 people. . . . So I'm not really in a position to say – to somehow apply that in reverse. The research, I'm sorry, just wasn't designed to be used in that way and I – I couldn't in good conscience respond to that." **)** (emphasis added).

457. Van Dyke does not explain why none of the individuals notified by LabMD that their PII (Personal Identifying Information) had been disclosed to unauthorized persons became victims of identity fraud. (RX 523 (Van Dyke, Dep. at 70-71)) (Q. ". . . So is it your opinion then that 30.5 percent of the individuals who were notified by LabMD that their personal identifying information had been disclosed to unauthorized persons will become victims of identity fraud?" A. "Yes." Q. "And hypothetically if none of those individuals became victim[s] of identity fraud are there any factors that come to mind that might cause that to happen?" A. "It's just impossible for me to speculate on something like that, it just defies reason." Q. "Well, it would defy reason at least in your mind that that could even happen, wouldn't it?" A. "Yes.").

458. Van Dyke "assumed that LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks." (Van Dyke, Tr. 642); (CX 0741 (Van Dyke, Rep. at 2)).

459. Van Dyke assumed that the 1718 File and the Sacramento Day Sheets were found outside of LabMD as a result of a data breach. (Van Dyke, Tr. 678-679).

PUBLIC

460. Van Dyke is not a statistician, yet his report relied upon a cross-tabulation technique which involves "comparison of statistical data." (Van Dyke, Tr. 673-675); (Van Dyke, Tr. 587) (Q. "Do you use cross-tabulation?" A. "Yes. Yeah. I might have -- it might be easier if I just said the method I was describing a moment ago was cross-tabulation." Q. "And what is cross-tabulation?" A. "So that's a -- within the research circle, that's a term that's widely used to describe statistical -- you know, comparison of statistical data.").

461. Van Dyke's definition of cross–tabulation is confusing and inconsistent. (Van Dyke, Tr. 587) (Cross–tabulation is the "comparison of statistical data."); (A. ". . . Cross-tabulation is just a universally accepted method among researchers for comparing two populations, people who have experienced two things. However, it is the same thing. . . .").

462. In reference to Figure 1 at page 8 of his report in this case, Van Dyke confuses cross–tabulation comparing data from selected survey years with cross–tabulation of data within a single survey year, which renders his testimony self–contradictory and unreliable. (Van Dyke, Tr. 650-651) (Q. "And in terms of utilizing cross-tabulation, do you do that to arrive at conclusions on the same survey or do you take information over a period of years and cross-tabulate it to come to conclusions?" A. "Oh. We would never -- if I'm understanding your question, we would never compare the results of individuals who respond in a particular way to -- within one survey -- and I need to be very careful about the way I'm communicating this -- with a set of respondents from another survey. In other words, we wouldn't mash the data together, so to speak. . . . Cross-tabulations were done within [Fig. 1 of my report], and we compared the results of that cross-tabulation to the results of a cross-tabulation in another survey." Q. "So another survey of the same kind for a different year." A. "Yes." Q. "Because if you look at figure 1, it appears that there's years 2010, 2011, 2012 and 2013 listed there;

PUBLIC

correct?" A. "That's correct." Q. "So are you saying that these numbers for each year are the result of a cross-tabulation?" A. "Within each year."); (CX 0741 (Van Dyke, Rep. at 8 (Fig. 1)).

463. Van Dyke testified that cross–tabulation and extrapolation "are different things" and extrapolation is "more accurate" in his opinion. (Van Dyke, Tr. 673-674) (JUDGE CHAPPELL: "What's the difference in cross-tabulation and extrapolation?" THE WITNESS: "Yeah, those are different things. So extrapolation is a process of reaching a conclusion, and so it might include just logic or just a wide variety of methods. But cross-tabulation is a statistician's method of precisely comparing, taking a subset of another, essentially doing division." JUDGE CHAPPELL: "Which is more accurate?" THE WITNESS: "A cross-tabulation would be more accurate, Your Honor." BY MR. SHERMAN: Q. "But you're not a statistician; correct?" A. "I'm not personally a statistician, no.").

464. Van Dyke never surveyed anyone from the 1718 File for purposes of his report, opinions, and testimony in this case. (Van Dyke, Tr. 677-678).

465. Van Dyke extrapolated the information in the 2013 Fraud ID Survey and overlaid data over the information from the 1718 File and the Sacramento Day Sheets. (Van Dyke, Tr. 676-677).

466. Van Dyke admitted that he never considered any of the specific facts of the case. (CX 0741 (Van Dyke, Rep. at 72-73)).

467. Van Dyke did not account for type of breach or who gained the information. (RX 523 (Van Dyke, Dep. at 42-43, 58)).

468. Van Dyke assumed that the same amount of damage would occur from the disclosure of the information regardless of how long it was available on a peer to peer network. (RX 523 (Van Dyke, Dep. at 41)).

L. <u>Professor Shields.</u>

469. Complaint Counsel did not proffer an expert witness with respect to P2P networks or LimeWire. (Tr. 747-748).

470. Professor Clay Shields ("Shields") testified as a rebuttal witness *only*. (Tr. 747-748).

471. Shields confirmed Fisk's testimony that once an ultrapeer discovers that another peer (computer) is behind a firewall, which it finds out when it initially runs a search, the ultrapeer is "able to test its network connection and determine if there's a firewall. If it determines there's a firewall, it finds . . . [another of the] ultra peers that's outside the firewall that's able to act on its behalf." (Shields, Tr. 841-842) (confirming Fisk's expert testimony).

472. Professor Shields was not able to find the 1718 File on the Gnutella network as he wrote his rebuttal expert report or prepared to testify. (Shields, Tr. 892).

473. Professor Shields does not have much, if any, experience with LimeWire. (Shields, Tr. 893).

474. Professor Shields does not know how the LabMD 1718 File was "actually shared," obtained by Tiversa, or if or how the 1718 File got on the network. (Shields, Tr. 904-07).

475. Professor Shields' opinions were based on the deposition of Boback and he assumed that the 1718 File had been shared and made available over Gnutella on the LimeWire network. (Shields, Tr. 904-06).

476. Computers with firewalls cannot be ultrapeers. (Shields, Tr. 909).

477. Finding one particular file on the internet by use of LimeWire is sort of like the lottery. (Shields, Tr. 917).

PUBLIC

478. A file, like the 1718 File, that includes the lettered series of "insuranceaging" cannot be found by a LimeWire search for the term "insurance." (Shields, Tr. 917-18).

M. <u>Complaint Counsel's Proofs</u>.

479. There is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); (RX 524 (Hill, Dep. at 149)).

480. Complaint Counsel introduced any evidence that any of LabMD's alleged unfair data security acts or practices, even taken together, "causes" substantial injury to consumers or harm to competition. (Tr. 1-1486); (CX 0001 – CX 0878).

481. Complaint Counsel has not introduced any evidence that LabMD's pre-July 2010, data security acts or practices are continuing or that such wholly past acts or practices "likely to cause" future harm, almost six years after the fact. (Tr. 1-1486); (CX 0001 – CX 0878).

482. Complaint Counsel has not introduced any evidence or proven that the 1718 File has been obtained by anyone other than Tiversa, Johnson, Dartmouth and FTC, or that it was available via LimeWire at LabMD after May 2008, approximately seven and one-half years ago. (Tr. 1-1486); (CX 0001 – CX 0878).

483. The 1718 File was taken by Tiversa on February 25, 2008, and subsequently disclosed to Johnson, Dartmouth and FTC. (Wallace, Tr. 1441-1442, 1358-1364); (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 8, 11-12)).

485. The 1718 File was not obtained, reviewed, or disclosed by any other person, except by the intentional actions of Boback, Wallace, Tiversa, Johnson, Dartmouth, and FTC. (Wallace, Tr. 1441-1442, 1358-1364); (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 8, 11-12)).

PUBLIC

486. The 1718 File was not available via LimeWire from LabMD after May 2008. (RX 097 – RX 118 (Daily IT Walk) (May 2008 – July 2008); (RX 119 – RX 169 (LabMD email re: walk arounds) (Mar. 2009 – Aug. 2009); (RX 174 – RX 264 (LabMD email re: walk arounds) (Aug. 2007 – July 2008)).

484. No consumer has suffered monetary or reputational harm due to the "Security Incidents" described in the Complaint. (Tr. 1-1486); (CX 0001 – CX 0878).

485. Complaint Counsel has not introduced evidence that consumers who receive notice of a data breach not reasonably capable of mitigating the injury. (Tr. 1-1486); (CX 0001 – CX 0878).

486. Complaint Counsel seeks to declare wholly past conduct in this case unfair and unlawful. (Complaint (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357), at 1-12 ¶¶ 1-23, Appendix A (13-57)).

487. Complaint Counsel did not introduce any evidence the allegation in ¶4 of the Complaint, that "[c]onsumers ***in many instances*** pay respondent's charges with credit cards or personal checks" is now true or was so with regard to any of the specific individuals in the 1718 File or the Day Sheets. (Tr. 1-1486); (CX 0001 – CX 0878).

489. Complaint Counsel did not introduce any evidence regarding the allegation in ¶6 of the Complaint, that LabMD "routinely obtains information about consumers," is now true. The evidence is LabMD has not obtained information about consumers since January, 2014. (CX0291 (LabMD Letter to Physicians Offices re: Closing); (Tr. 1-1486); (CX 0001 – CX 0878)).

490. LabMD does not operate a computer network. (CX0291 (LabMD Letter to Physicians Offices re: Closing)).

PUBLIC

491. LabMD's billing department does not use the computer networks to generate or access documents related to processing copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers. (CX0291 (LabMD Letter to Physicians Offices re: Closing)).

492. Complaint Counsel did not introduce any evidence regarding the allegation in ¶10 of the Complaint that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." (Tr. 1-1486); (CX 0001 – CX 0878).

493. LabMD used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. (RX 533 (Fisk, Rep. at 3-4, 6-34, 37); (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3 ("***Factors that determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources.***") (emphasis added), 12 (***"The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts."***) (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20,

PUBLIC

2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)); (Dep't of Health & Human Servs. (HIPAA Security Series (**6 Basics of Risk Analysis and Risk Management**) (Volume 2/ Paper 6) (6/2005: rev. 3/2007), 3)) ("…only federal agencies are required to follow federal guidelines like the NIST 800 series … Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.") (italic emphasis in original) (bold emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf (last accessed Aug. 9, 2015)).

494. LabMD required employees and doctors to use common authentication-related security measures. (RX 533 (Fisk, Rep. at 16-22); (RX 071 (LabMD Employee Handbook); (CX 0005 (LabMD Compliance Program); (RX 075 – RX 095 (LabMD Acceptable Use and Security Policy); (CX 0130 (LabMD Employee Handbook)).

495. Complaint Counsel did not introduce any evidence regarding the allegation in ¶11 of the Complaint that LabMD "could have corrected its security failures at relatively low cost using readily available security measures." (Tr. 1-1486); (CX 0001 – CX 0878).

496. Complaint Counsel did not introduce any evidence regarding the allegation in ¶12 of the Complaint that LabMD's "[c]onsumers have no way of ***independently knowing*** about respondent's [alleged] security failures and ***could not reasonably avoid possible harms*** from such [alleged] failures, including identity theft, medical identity theft, and other harms, such as

PUBLIC

disclosure of sensitive, private medical information." (Tr. 1-1486); (CX 0001 – CX 0878) (emphasis added).

497. LabMD is subject to the HIPAA Breach Notification Rule and has complied with it in the past – the FTC has admitted that LabMD has always complied with HIPAA/HITECH data-security standards. (CX 0679 *(LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), Ex. 12 at p. 13)).

498. Complaint Counsel offered no testimony or other evidence this Rule was inadequate. (Tr. 1-1486); (CX 0001 – CX 0878).

499. The Commission did not warn businesses about the risk of inadvertent file sharing until January 2010, at the earliest. (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

500. The 1718 File was not generally available on a P2P network through LimeWire, a P2P file sharing application. (Wallace, Tr. 1361-1444); (Fisk, Tr. 1153) ("So in the case of the insurance aging file, . . . [the program was] not intelligent enough to separate 'insurance' from 'aging,' so it [would] just take 'insurance' -- it [would] see that underscore and it [would see] 'insuranceaging' as one big keyword, and then it [would] actually do what's called a little bit of prefix matching on that, on that keyword. So once it's identified 'insuranceaging' as a keyword, it [would] then strip off the final characters of up to three, so it [would] enter 'insuranceaging' as the keyword, and then it will enter 'insuranceagin' without the 'g' and then 'insuranceagi' without the 'n' and the 'g' and 'insuranceag' without the 'ing' as all – as separate, as separate keywords. And then it [would] also enter the numbers as keywords as well."); (Fisk, Tr. 1156).

PUBLIC

498. Complaint Counsel offered no testimony that consumers, upon receiving notice, were anything other than reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact. (Tr. 1-1486); (CX 0001 – CX 0878).

499. Complaint Counsel did not introduce any evidence regarding the allegation in ¶15 of the Complaint that "[g]enerally, once shared, a file cannot with certainty be removed permanently from a P2P network." (Tr. 1-1486); (CX 0001 – CX 0878).

500. Complaint Counsel did not introduce any evidence regarding the allegation in ¶16 of the Complaint that "[s]ince at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks." (Tr. 1-1486); (CX 0001 – CX 0878).

502. The Commission did not warn businesses about the risk of inadvertent file sharing until January 2010. (Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 10, 40-84 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015) ("The [2005 FTC Report] emphasized that many of the risks posed by P2P file sharing also exist when consumers engage in other Internet-related activities, such as surfing Web sites, using search engines, or e-mail.…")); (FTC Staff Report, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, 20 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015) ("***Although it has required warnings with respect to inherently dangerous products, the Commission concluded that it was not aware of any basis under the FTC Act for requiring warnings for P2P file sharing and other neutral consumer***

PUBLIC

technologies.") (emphasis added); (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

501. Complaint Counsel has failed to prove by a preponderance of the evidence the allegations in ¶¶17-18 of the Complaint that LabMD's insurance aging file was generally available on a P2P network through Limewire, a P2P file sharing application. (Wallace, Tr. 1361-1444).

502. LabMD did not knowingly violate Section 5. (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (Daugherty, Tr. 985-987)).

503. Complaint Counsel has not alleged or proven LabMD is a serial violator of Section 5. (Tr. 1-1486); (CX 0001 – CX 0878).

504. FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices, stating that LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

505. FTC did not name an individual complainant or allege direct harm to any identifiable person, and FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively

PUBLIC

low cost." (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

506. FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," and at any given point in time, allegedly violated Section 5. (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

N. <u>The Damage Done To LabMD</u>

507. LabMD provided a unique, useful and important service to doctors and their

patients. (Daugherty, Tr. 493, 944-945, 955-964); (Daugherty, Tr. 962) (A. "And in our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices. . . . the amount of errors just fell through the floor. . . . [W]e even knew ahead of time what was coming so that we could be prepared.").

508. The Commission's inquisition substantially interfered with LabMD's operations.

(Daugherty, Tr. 1028-1034).

509. LabMD criticized FTC and Commission staff. (Respondent LabMD's Motion to

Dismiss the Complaint With Prejudice (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357) at 30 n.23)) ("Notably, the Complaint (along with a FTC press release making disparaging

PUBLIC

claims about LabMD) was issued shortly before publication of LabMD's CEO's book, *The Devil Inside the Beltway*, in which he exercises his First Amendment right to speak candidly about a matter of public concern and criticizes Complaint Counsels' actions and the Commission's treatment of LabMD in great detail. Complaint Counsels' burdensome and oppressive discovery requests—which run afoul of norms of conduct that obtain in Article III courts and *flagrantly* violate Fed. R. Civ. P. 30(a)(2)(A)'s limits on depositions—followed shortly after the book's publication. The First Amendment prohibits government agencies from retaliating against private citizens for engaging in constitutionally protected speech by bringing baseless enforcement actions. *See Trudeau v. FTC*, 456 F.3d 178, 190-91 nn.22-23 (D.C. Cir. 2006))." (emphasis in original).

510. The Commission brought a complaint against LabMD in August, 2013, after LabMD had publicly criticized FTC and its staff in very strong terms. (Daugherty, Tr. 1027).

511. At that time [August 2013], the Commission did not have evidence that any consumer had suffered monetary harm or other harm due to the Security Incidents. (Complaint, *In the Matter of LabMD, Inc., a corporation*, at 1-12, Appendix A (13-57)).

512. At that time, the Commission did not have evidence LabMD's post July, 2010, data security acts or practices were inadequate or unreasonable. (Complaint, In the Matter of LabMD, Inc., a corporation, at 1-12, Appendix A (13-57)).

513. LabMD's pre-July 2010 data security acts or practices changed over time and could not reoccur. (Tr. 1-1486); (CX 0001 – CX 0878).

PUBLIC

514. In or about August 2013, the Commission knew or should have known that the

1718 File had been obtained only by and was available only to Tiversa, Johnson, Dartmouth and FTC. (Complaint, In the Matter of LabMD, Inc., a corporation, at 1-12, Appendix A (13-57)).

515. For three and one-half months, Commission staff did not inform LabMD that FTC had possession of the Day Sheets. However, Commission staff knew or should have known LabMD had an obligation under HIPAA to give notice of the unauthorized disclosure of PHI or PII. (Daugherty, Tr. 1027-1028) (Q. **"**What is it that you contend that the Federal Trade Commission didn't tell you?" A. "They didn't tell us they had the day sheets for three and a half months, even though we're subject to HIPAA, which requires us to notify in 60 days. . . . On the one hand we're supposed to protect patients and we're supposed to follow the law, and yet the federal government is withholding information from us, so it seems to me they're more eager to lambaste us and entrap us than keep patients safe. So we were outraged, scared, felt entrapped, and employees were starting to really break under pressure when that went down.").

516. FTC's actions in this case destroyed morale, attention, and energy at LabMD. (Daugherty, Tr. 1028) (Q. **"**What other impacts did it have on LabMD's business?" A. ". . . I can't understate how damaging and confusing and sideswiping this was to the attention, energy and morale of the management staff that knew because we, you know, had a company to run....").

517. FTC's actions in this case destroyed LabMD's client base generally by attrition and innuendo, and specifically by Complaint Counsel's serving subpoenas upon and deposing LabMD's employees, clients, client–physicians, and third–party vendors. (Daugherty, Tr. 1029-1031) (Q. "Was there any impact on the business externally?" A. "Yes." Q. "And what was

PUBLIC

that?" A. "Well, the press broke the story in 2012, so once the press broke the story, . . . you can't control perception, and so I had physicians upset with me they didn't hear it from myself. I had people concerned . . . The negative external impact on LabMD's business reputation, income, and ability to keep and maintain clients, employees, and third-party vendors was exacerbated by the fact that "most people in medicine don't know what the FTC is" because the FTC does not regulate data security or anything else in the medical industry."); (Daugherty, Tr. 1029-1030) (Q. "Was there any impact on the business externally?" A. "Yes." Q. "And what was that?" A. ". . .I did find out later, for example, the rumor had twisted around so that -- because, you know, most people in medicine don't know what the FTC is, so I'm getting told, I hear you're in trouble with the SEC about some trade -- I mean, just the rumors just went crazy.").

518. In or about November 13, 2013, however, Commission staff knew or should have

known Tiversa and Boback had committed perjury with respect to claims of spread reflected on CX 0019. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found); (Wallace, Tr. 1344-1347, 1352-1354, 1358-1374, 1378-1385)).

519. As of May 27, 2014, LabMD's operations were operational only for the purposes of maintaining tissue samples for LabMD's physician-clients and the patients they jointly serve. (Daugherty, Tr. 1031) (Q. "Mr. Daugherty, what is the current state of LabMD's operations?" A. "LabMD is in a very deep coma. We are still in business. The corporation is still standing. I'm the only employee. All we do -- we preserve the slides and the electronic data for the physicians so they can still get results if they don't have them and they can still send slides out

PUBLIC

for second opinions. Because that goes on, you know, that doesn't just stop. . . . prostate cancer is a very slow-growing disease, so you can have it for 14 years, . . . and there's technologies [that are] available now to analyze versus what was available five years ago [on] aggressiveness of the tumor cells, so we keep all that available still."); (CX 0291 (LabMD Letter to Physicians' Offices re: Closing) (". . . First and foremost, even during this closure, patient care is still priority number one with LabMD . . .")).

520. As a result of FTC's actions in this case, LabMD was sued by its landlord for approximately $900,000.00 for early termination of its lease. (Daugherty, Tr. 1031-1032).

521. As a result of FTC's actions in this case, LabMD has lost all primary insurance coverage for its employees as well as its malpractice insurance for both LabMD's physician–employees and its facility. (Daugherty, Tr. 1032-1033) (Q. "What's the state of LabMD's insurance coverage?" A. "Well, in the beginning, we of course had medical insurance, dental insurance, workmen's comp, vision, general liability, medical malpractice for the physicians, medical malpractice for the facility. So of course we had to let everybody go. They still have dental and medical through COBRA should they choose at their expense. The vision is gone. The workmen's comp is gone. . . . [The] general liability for the corporation has been nonrenewed because of the Federal Trade Commission action and claims.[]" Q. "How do you know that's the reason?" A. "Because they told us. The medical malpractice -- when you close -- obviously we're not practicing medicine now and moving forward, so the medical malpractice is for tail coverage for any claims -- any claims from any practiced medicine we did in the last few years would be covered in the future for the next couple of years. We had carriers that flat-out would deny to quote us because of the Federal Trade Commission investigation, even though, you know, these are medical malpractice. I don't think that the Federal Trade

PUBLIC

Commission has any jurisdiction over medical malpractice. . . . but [the malpractice carriers] didn't care. . . . I got tail coverage for the physicians, and there were many fewer insurance carriers that were willing to quote it. But we did get insurance [] tail coverage for the two physicians that we had to let go.").

522. As a result of the FTC's actions in this case, LabMD sent a letter dated January 6, 2014 to its administrators, physicians, nurses, and "valuable support staff" stating that the last day patient specimens would be accepted at the facility would be Saturday, January 11, 2014. (CX 0291 (LabMD Letter to Physicians Offices re: Closing)) (". . . It is with deep regret and sadness I am writing you to announce that the last day LabMD will be accepting new specimens is Saturday, January 11, 2014. . . .").

523. In its letter dated January 6, 2014, LabMD stated that the reason for its actions in shutting down its facility was "the conduct of the [FTC]" in that the FTC's actions "subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data–security vulnerability." (CX 0291 (LabMD Letter to Physicians Offices re: Closing)) ("The FTC has subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data–security vulnerability. Without standards, information, or Congressional approval, and without a customer victim from the alleged 'breach,' the FTC has taken it upon itself to spend your tax dollars to ruin LabMD and regulate medical data security over and above HIPAA. LabMD's fight with the FTC has become, as Government Health IT stated, ". . . a dispute that could shape the future of health privacy regulation.' In other words, this is a very big deal that may result in another regulator, without expertise or clear standards, standing over your shoulder with the power to destroy your practice or your company.")

/s/ Daniel Z. Epstein
Daniel Z. Epstein
Prashant K. Khetan
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW Suite 650
Washington, DC 20006
Phone: (202) 499-4232
Facsimile: (202) 330-5842
Email: daniel.epstein@causeofaction.org

Counsel for Respondent

/s/ *Reed D. Rubinstein*
Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Facsimile: (202) 372-9141
Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

PUBLIC

CERTIFICATE OF SERVICE

I hereby certify that on August 11, 2015, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

Donald S. Clark, Esq.
Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW, Rm. H-113
Washington, DC 20580

I also certify that I delivered via hand delivery and electronic mail copies of the foregoing document to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Ave., NW, Rm. H-110
Washington, DC 20580

I further certify that I delivered via electronic mail a copy of the foregoing document to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Ryan Mehm, Esq.
John Krebs, Esq.
Jarad Brown, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Room CC-8232
Washington, DC 20580

Dated: August 11, 2015 /s/ Patrick J. Massari

PUBLIC

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: August 11, 2015 /s/ Patrick J. Massari

ATTACHMENT 1

IN THE MATTER OF
LABMD, INC
DOCKET NO. 9357

RESPONDENT COUNSEL'S EXHIBIT INDEX

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX001	6/1/07 Day Sheet Transaction Details	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1011; 1013-1019; 1021-1033; 1071-1078		CX0687
RX002	Insurance company web access sheet	JX 2 see Tr. 6:15-16			
RX003	IT Staff Checklist	JX 2 see Tr. 6:15-16			
RX004	website list	JX 2 see Tr. 6:15-16			
RX005	windows screenshot	JX 2 see Tr. 6:15-16			
RX006	Sentinel Network Complaint	JX 2 see Tr. 6:15-16			CX0402
RX007	FTC envelop scan	JX 2 see Tr. 6:15-16			CX0441
RX008	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0491
RX009	Service Solutions Proposal for LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0047
RX010	Email from H. Davidson to M. Daugherty dated	JX 2 see Tr. 6:15-16			
RX011	Service Solutions Proposal for LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX012	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX013	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0048
RX014	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0049
RX015	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0050
RX016	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX017	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX018	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX019	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX020	Service Solutions Proposal for LabMD from ProviDyn	JX 2 see Tr. 6:15-16			
RX021	Service Solutions Proposal for LabMD from ProviDyn	JX 2 see Tr. 6:15-16			CX0051
RX022	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0055
RX023	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX024	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0057
RX025	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0059
RX026	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0061

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX027	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0062
RX028	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0063
RX029	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0064
RX030	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0065
RX031	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX032	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX033	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX034	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX035	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX036	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX037	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0066
RX038	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0072
RX039	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0073
RX040	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0074
RX041	Email from J. Boyle to R. Boback re: Breach Notification	JX 2 see Tr. 6:15-16			
RX042	Rapid SSL ad	JX 2 see Tr. 6:15-16			CX0135
RX043	Rapid SSL FAQ	JX 2 see Tr. 6:15-16			
RX044	TrendMicro ad	JX 2 see Tr. 6:15-16			
RX045	Cyprus Communications Services Order	JX 2 see Tr. 6:15-16			CX0253
RX046	Managed Data Solutions Invoice	JX 2 see Tr. 6:15-16			CX0264
RX047	MediPro Sale Invoices	JX 2 see Tr. 6:15-16			
RX048	MediPro Sales Invoice	JX 2 see Tr. 6:15-16			
RX049	MediPro Sales Invoice	JX 2 see Tr. 6:15-16			
RX050	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX051	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX052	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16	Daugherty, Tr. 985-987		
RX053	Email between Boyle, Daugherty, and Tiversa	JX 2 see Tr. 6:15-16			
RX054	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX055	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX056	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX057	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX058	Email between Boyle and Daugherty re: breach	JX 2 see Tr. 6:15-16			
RX059	Email between Boyle and Tiversa re: breach	JX 2 see Tr. 6:15-16			
RX060	Mail Batch Instructions	JX 2 see Tr. 6:15-16			CX0162
RX061	Daily Credit Card Transactions Form	JX 2 see Tr. 6:15-16			CX0233
RX062	LabMD New Team Member Checklist	JX 2 see Tr. 6:15-16			CX0003

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX063	Patient Aging Report	JX 2 see Tr. 6:15-16			CX0163
RX064	Rose Bellvue 2008 Performance eval	JX 2 see Tr. 6:15-16			
RX065	LabMD Staff Responsibility breakdown	JX 2 see Tr. 6:15-16			CX0234
RX066	Jan 2007 Monthly Status of Pending Tasks Form	JX 2 see Tr. 6:15-16			CX0119
RX067	List of clients with remote access to LabMD system	JX 2 see Tr. 6:15-16			CX0134
RX068	LabMD Performance Eval Form	JX 2 see Tr. 6:15-16			
RX069	LabMD Insurance Aging Report	JX 2 see Tr. 6:15-16			CX0165
RX070	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0005
RX071	LabMD Employee Handbook	JX 2 see Tr. 6:15-16	Hill, Tr. 288-295		
RX072	LabMD Insurance Aging Report (1718 file)	JX 2 see Tr. 6:15-16			CX0166
RX073	Certification page signed by Daugherty	JX 2 see Tr. 6:15-16			
RX074	LabMD Computer Hardware and Security Manual	JX 2 see Tr. 6:15-16			
RX075	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX076	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX077	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX078	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX079	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX080	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX081	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX082	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX083	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX084	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX085	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX086	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX087	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX088	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX089	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX090	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX091	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX092	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX093	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX094	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX095	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX096	Server Ports and Firewall Mapper	JX 2 see Tr. 6:15-16			CX0178
RX097	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX098	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX099	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX100	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX101	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX102	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX103	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX104	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX105	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX106	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX107	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX108	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX109	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX110	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX111	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX112	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX113	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX114	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX115	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX116	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX117	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX118	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX119	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX120	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX121	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX122	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX123	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX124	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX125	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX126	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX127	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX128	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX129	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX130	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX131	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX132	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX133	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX134	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX135	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX136	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX137	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX138	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX139	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX140	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX141	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX142	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX143	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX144	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX145	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX146	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX147	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX148	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX149	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX150	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX151	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX152	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX153	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX154	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX155	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX156	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX157	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX158	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX159	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX160	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX161	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX162	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX163	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX164	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX165	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX166	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX167	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX168	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX169	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX170	TrendMicro Daily Virus Report	JX 2 see Tr. 6:15-16			CX0185
RX171	LabMD Virus Log	JX 2 see Tr. 6:15-16			
RX172	LabMD Policy Manual	JX 2 see Tr. 6:15-16			CX0006
RX173	LabMD IT Staff Walkaround Checklist	JX 2 see Tr. 6:15-16			CX0004
RX174	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX175	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX176	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX177	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX178	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX179	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX180	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX181	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX182	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			CX0236
RX183	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX184	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX185	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX186	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX187	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX188	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX189	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX190	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX191	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX192	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX193	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX194	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX195	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX196	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX197	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX198	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX199	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX200	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX201	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX202	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX203	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX204	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX205	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX206	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX207	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX208	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX209	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX210	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX211	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX212	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			CX0199
RX213	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX214	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX215	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX216	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX217	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX218	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX219	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX220	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX221	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX222	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX223	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX224	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX225	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX226	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX227	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX228	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX229	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX230	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX231	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX232	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX233	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX234	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX235	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX236	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX237	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX238	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX239	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX240	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX241	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX242	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX243	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX244	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX245	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX246	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX247	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX248	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX249	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX250	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX251	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX252	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX253	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX254	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX255	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX256	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX257	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX258	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX259	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX260	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX261	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX262	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX263	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX264	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX265	ZyXel Firewall Rules Storage Space in Use	JX 2 see Tr. 6:15-16			CX0257
RX266	LabMD Server Room Security Chart - Jun 2010	JX 2 see Tr. 6:15-16			
RX267	LabMD Server Room Security Chart - Jul 2010	JX 2 see Tr. 6:15-16			
RX268	Malware Quickscan Log	JX 2 see Tr. 6:15-16			CX0268
RX269	Malware Quickscan Log	JX 2 see Tr. 6:15-16			CX0818
RX270	Malware Bytes Scanner	JX 2 see Tr. 6:15-16			
RX271	Security scan results	JX 2 see Tr. 6:15-16			CX0825
RX272	Security Scan Results	JX 2 see Tr. 6:15-16			CX0830
RX273	Product Key Chart	JX 2 see Tr. 6:15-16			CX0169
RX274	July 2010 Security Scan List	JX 2 see Tr. 6:15-16			CX0193
RX275	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX276	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX277	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX278	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX279	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX280	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX281	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX282	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX283	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX284	Desktops/Servers Virus Summary	JX 2 see Tr. 6:15-16			
RX285	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX286	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX287	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX288	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX289	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX290	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX291	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX292	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX293	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX294	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX295	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX296	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX297	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX298	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX299	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX300	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX301	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX302	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX303	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX304	Malware Quickscan Log	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX305	LabMD Employee Separation Agreement - Patrick Howard	JX 2 see Tr. 6:15-16			
RX306	Automated PC Technologies New Service Agreement	JX 2 see Tr. 6:15-16			CX0395
RX307	APT Service Invoice	JX 2 see Tr. 6:15-16			CX0035
RX308	Christopher Maire resume	JX 2 see Tr. 6:15-16			CX0203
RX309	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0005
RX310	LabMD Compliance Training Powerpoint	JX 2 see Tr. 6:15-16			CX0127
RX311	LabMD Employee Handbook acknowledgment page-Woodson	JX 2 see Tr. 6:15-16			
RX312	Email between Sandra Brown and John Boyle re: Limewire issues	JX 2 see Tr. 6:15-16			CX0170
RX316	Pathology Records and Materials Retention	JX 2 see Tr. 6:15-16			CX0834
RX317	Managed Data Solutions Security Scan Summary	JX 2 see Tr. 6:15-16			CX0046
RX318	LabMD connections map for Power Ferry Rd location- 2009	JX 2 see Tr. 6:15-16			CX0039
RX319	LabMD connections map for Power Ferry Rd location- 2010	JX 2 see Tr. 6:15-16			CX0040
RX320	LabMD connections map for Power Ferry Rd location- 2011	JX 2 see Tr. 6:15-16			CX0041
RX321	Juniper Networks Product Descriptions	JX 2 see Tr. 6:15-16			CX0835
RX322	Brandon Bradley resume	JX 2 see Tr. 6:15-16			CX0320
RX323	Monthly Computer Inspection Report	JX 2 see Tr. 6:15-16			
RX324	LabMD Serverroom virus scan - July 2010	JX 2 see Tr. 6:15-16			
RX325	Managed Data Solutions Project Proposal	JX 2 see Tr. 6:15-16			CX0194
RX326	Managed Data Solutions Project Proposal	JX 2 see Tr. 6:15-16			CX0195
RX327	Tiversa folder screenshot	JX 2 see Tr. 6:15-16			CX0149; CX CX0151; CX
RX328	LabMD folder screenshot	JX 2 see Tr. 6:15-16			CX0153
RX329	Limewire screenshot	JX 2 see Tr. 6:15-16			CX0154; CX CX0156
RX330	Insurance Aging pdf window screenshot	JX 2 see Tr. 6:15-16			CX0157
RX331	SacPD Netanalysis re: Maldonado and Garcia	JX 2 see Tr. 6:15-16			CX0101
RX332	Letter to M. Cox from R.J. Maxay	JX 2 see Tr. 6:15-16			CX0225
RX333	Letter to M. Cox from A.C. Troutman	JX 2 see Tr. 6:15-16			
RX334	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0129
RX335	Confidentiality Agmt. Between LabMD and Deanna Bagwell Dated 3/23 (no year)	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX336	LabMD Employee Handbook	JX 2 see Tr. 6:15-16			CX0130
RX337	Form Letter from LabMD to affected patients	JX 2 see Tr. 6:15-16			
RX338	Handbook Receipt Signed By Adnan Savera	JX 2 see Tr. 6:15-16			
RX339	Email From J. Boyle To mdort@aol.com	JX 2 see Tr. 6:15-16			
RX340	Emai From J. Boyle To mikelabmd@gmail.com; mdort@aol.com	JX 2 see Tr. 6:15-16			
RX341	Email From G. Schultz to R. Boback	JX 2 see Tr. 6:15-16			
RX342	Email from J. Boyle to W. Hardin re: Preventative Maintenance	JX 2 see Tr. 6:15-16			
RX343	Email from W. Hardin to J. Boyle re: preventative maintenance	JX 2 see Tr. 6:15-16			
RX344	LabMD "Network Invent" summary	JX 2 see Tr. 6:15-16			CX0397
RX345	Automated PC Technologies Invoice	JX 2 see Tr. 6:15-16			CX0398
RX346	Email from R. Yodaiken to K. Jestes re: contact with the FBI	JX 2 see Tr. 6:15-16			
RX347	Email from K. Jestes to M. Wood re: RedactedLabMdsLetter	JX 2 see Tr. 6:15-16			
RX348	LabMD Patient Notification Letter [redacted]	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1019-1021		
RX349	Email from A. Sheer to K. Jestes re: Hi Karina - The package arrived safe and sound. Alain.	JX 2 see Tr. 6:15-16			
RX350	Email from K. Jestes to A. Sheer re: LabMD	JX 2 see Tr. 6:15-16			
RX351	Email from A. Sheer to K. Jestes re: LabMD from Sacrameno Police	JX 2 see Tr. 6:15-16			
RX352	Email from R. Yodaiken to K. Jestes re: LabMD	JX 2 see Tr. 6:15-16			
RX353	Email from R. Yodaiken to K. Jestes re: my first phone call	JX 2 see Tr. 6:15-16			
RX354	Email from A. Sheer to K. Jestes re: my first phone call	JX 2 see Tr. 6:15-16			
RX355	Clinical Laboratory Licenses	JX 2 see Tr. 6:15-16			
RX356	Unofficial protocol for document transmission between LabMD and Midtown Urology	JX 2 see Tr. 6:15-16			
RX357	LabMD closure announcement	JX 2 see Tr. 6:15-16			
RX358	LabMD Billing Patient Education article	JX 2 see Tr. 6:15-16			
RX359	Fusco Letter to Dartmouth	JX 2 see Tr. 6:15-16			
RX360	S. Fusco Letter to E. Johnson	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX361	S. Fusco Letter to Tiversa	JX 2 see Tr. 6:15-16			
RX362	LabMD IT project outline	JX 2 see Tr. 6:15-16			CX0313
RX363	Email from J. Boyle to M. Daugherty re: Your Passwords	JX 2 see Tr. 6:15-16			
RX364	J. Boyle email to M. Daugherty re: Hyer Software request	JX 2 see Tr. 6:15-16			
RX365	Email from C. Gormley to E. Johnson re: Aids clinic ppt	JX 2 see Tr. 6:15-16			
RX366	Aids clinic names/ssn chart	JX 2 see Tr. 6:15-16			
RX367	Email from C. Gormley to E. Johnson re: Are you...	JX 2 see Tr. 6:15-16			
RX368	Email from C. Gormley to E. Johnson re: Files	JX 2 see Tr. 6:15-16			
RX369	Email from C. Gormley to E. Johnson re: Medical Insurance Terms	JX 2 see Tr. 6:15-16			
RX370	Johnson/Tiversa Medical Insurance Terms List	JX 2 see Tr. 6:15-16			
RX371	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX372	Email from C. Gormley to E. Johnson re: link	JX 2 see Tr. 6:15-16			
RX373	Email from C. Gormley to E. Johnson re: link	JX 2 see Tr. 6:15-16			
RX374	Email from C. Gormley to E. Johnson re: post-release	JX 2 see Tr. 6:15-16			
RX375	Email from C. Gormley to E. Johnson re: are you..	JX 2 see Tr. 6:15-16			
RX376	Email from C. Gormley to E. Johnson re: fax of the revision should be arriving now	JX 2 see Tr. 6:15-16			
RX377	Email from C. Gormley to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX378	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX379	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX380	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX381	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX382	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX383	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX384	Email from C. Gormley to E. Johnson re: Link	JX 2 see Tr. 6:15-16			
RX385	Email from C. Gormley to E. Johnson re: pr	JX 2 see Tr. 6:15-16			
RX386	Email from C. Gormley to E. Johnson re: Public Hospital Footpring	JX 2 see Tr. 6:15-16			
RX387	Email from C. Gormley to E. Johnson re: Sending Over Thoughts	JX 2 see Tr. 6:15-16			
RX388	Email from C. Gormley to E. Johnson re: Sending Over Thoughts	JX 2 see Tr. 6:15-16			
RX389	Email from C. Gormley to E. Johnson re:	JX 2 see Tr. 6:15-16			
RX390	Email from E. Johnson to C. Gormley re:	JX 2 see Tr. 6:15-16			
RX391	Email from E. Johnson to C. Gormley re:	JX 2 see Tr. 6:15-16			
RX392	Email from E. Johnson to C. Gormley re: Dartmouth	JX 2 see Tr. 6:15-16			
RX393	Email from E. Johnson to C. Gormley re: Diagnostic Codes	JX 2 see Tr. 6:15-16			
RX394	Email from E. Johnson to C. Gormley re: Final Example	JX 2 see Tr. 6:15-16			
RX395	Email from E. Johnson to C. Gormley re: Medical Insurance Terms	JX 2 see Tr. 6:15-16			
RX396	Email from E. Johnson to C. Gormley re: Paper	JX 2 see Tr. 6:15-16			
RX397	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX398	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX399	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX400	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX401	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX402	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX403	E. Johnson emails and article re: data hemorrhaging	JX 2 see Tr. 6:15-16	Johnson, Tr. 783-785		

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX404	E. Johnson grant documents	JX 2 see Tr. 6:15-16	Sherman, Tr. 57; Johnson, Tr. 751-755		
RX405	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX406	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX407	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX408	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX409	LabMD Threat Scan	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1041-1042		
RX410	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX411	Communications between J.Parr and TrendMicro re:service	JX 2 see Tr. 6:15-16			
RX412	IT expenditure chart	JX 2 see Tr. 6:15-16			CX0683
RX413	Veritas Server Backup Report	JX 2 see Tr. 6:15-16			
RX414	Packet Filtering Summary	JX 2 see Tr. 6:15-16			
RX415	Kaloustian background check/A. Simmons' resignation	JX 2 see Tr. 6:15-16			
RX416	L. Hudson Termination Notice	JX 2 see Tr. 6:15-16			
RX417	Email: R. Yodaiken to K. Jestes, Subject: Contact with FBI	JX 2 see Tr. 6:15-16			
RX418	Email: L. Riposo VanDruff to K. Jestes, Subject: Courtesy copy of subpoena	JX 2 see Tr. 6:15-16			
RX419	Letter: L. Riposo VanDruff to K. Jestes	JX 2 see Tr. 6:15-16			
RX420	Email: D. Ojeda to ASHEER@ftc.gov	JX 2 see Tr. 6:15-16			
RX421	Email: K. Jestes to D. Ojeda, Subject:	JX 2 see Tr. 6:15-16			
RX422	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: Erick Garcia	JX 2 see Tr. 6:15-16			
RX423	Email: msmith4@ftc.gov to K. Jestes, Subject: File Request - Federal Trade Commission – File Request	JX 2 see Tr. 6:15-16			
RX424	Email: K. Jestes to M. Wood, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX425	Letter: (To: REDACTED) from M. Daugherty (No Subject)	JX 2 see Tr. 6:15-16			
RX426	Email: HELPDESK to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX427	Email: R. Yodaiken to K. Jestes, Subject: General ID theft -related information	JX 2 see Tr. 6:15-16			
RX428	Email: A. Sheer to K. Jestes, Subject: Hi Karina. The package arrived safe and sound - thanks. Alain	JX 2 see Tr. 6:15-16			
RX429	Email: A. Sheer to K. Jestes, Subject: LabMD (Attach: redacted LabMDs Letter(3.27.23).pdf)	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX430	Letter: (To: REDACTED) from M. Daugherty (No Subject)	JX 2 see Tr. 6:15-16			
RX431	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX432	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX433	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX434	Email: A. Sheer to K. Jestes, Subject: More id theft links	JX 2 see Tr. 6:15-16			
RX435	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX436	Email: R. Yodaiken to K. Jestes, Subject: our address	JX 2 see Tr. 6:15-16			
RX437	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX438	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX439	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX440	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX441	Email: A. Sheer to K. Jestes, Subject: Erick Garcia	JX 2 see Tr. 6:15-16			
RX442	Email: L. Riposo VanDruff to K. Jestes, Subject: follow up	JX 2 see Tr. 6:15-16			
RX443	Email: A. Sheer to K. Jestes, Subject: Hi Karina. The package arrived safe and sound - thanks. Alain	JX 2 see Tr. 6:15-16			
RX444	Email: R. Yodaiken to K. Jestes, Subject: Hi Karina. When you have a moment, could you send the tracking number? Thanks.	JX 2 see Tr. 6:15-16			
RX445	Email: A. Sheer to K. Jestes, Subject: Hi Karina. Would you have a few minutes to talk with us tomorrow (we're clear all day) o Wednesday (in the afternoon) to catch up? Thanks. Alain	JX 2 see Tr. 6:15-16			
RX446	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX447	Email: K. Jestes to A. Sheer, Subject: LabMD	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX448	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX449	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX450	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX451	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX452	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX453	Email: K. Jestes to A. Sheer, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX454	Email: A. Sheer to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX455	Email: A. Sheer to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX456	Email: R. Yodaiken to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX457	Email: L. Riposo VanDruff to K. Jestes, Subject: location for depo	JX 2 see Tr. 6:15-16			
RX458	Email: L. Riposo VanDruff to K. Jestes, Subject: location for depo	JX 2 see Tr. 6:15-16			
RX459	Email: R. Yodaiken to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX460	Email: A. Sheer to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX461	Email: A. Sheer to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX462	Email: K. Jestes to HELPDESK, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX463	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX464	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX465	Email: R. Yodaiken to A. Sheer and K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX466	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX467	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX468	Email: R. Yodaiken to K. Jestes, Subject: Sac County Courts online	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX469	Email: L. Riposo VanDruff to K. Jestes, Subject: subpoena results	JX 2 see Tr. 6:15-16			
RX470	Email: A. Sheer to K. Jestes, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX471	Email: A. Sheer to K. Jestes, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX472	Email: R. Yodaiken to K. Jestes, Subject: Update	JX 2 see Tr. 6:15-16			
RX473	Email: K. Jestes to R. Yodaiken, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX474	Email: R. Yodaiken to K. Jestes, Subject: sharing documents	JX 2 see Tr. 6:15-16			
RX475	Template (?) to General Counsel FTC, Subject: Request for Non-public Materials and Certification of Intent to Maintain Confidentiality and to Restrict Use to Law Enforcement Purposes	JX 2 see Tr. 6:15-16			
RX476	Email: A. Sheer to K. Jestes, Subject: Attach: 2013.08.27 Letter to Detective Jestes.PDF	JX 2 see Tr. 6:15-16			
RX477	Letter: A. Sheer to K. Jestes, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX478	Email: A. Sheer to K. Jestes, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX479	Email: K. Jestes to R. Yodaiken and A. Sheer, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX480	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: Update	JX 2 see Tr. 6:15-16			
RX481	LabMD Electronics Policy	JX 2 see Tr. 6:15-16			
RX482	Cyprus Master Terms	JX 2 see Tr. 6:15-16			
RX483	Emails between C. Gormley and E. Johnson Re: WSJ article	JX 2 see Tr. 6:15-16	Johnson, Tr. 770-775; 776-777		
RX484	Zhao/Johnson article	JX 2 see Tr. 6:15-16			
RX485	Tiversa press release	JX 2 see Tr. 6:15-16			
RX486	Deposition Transcript of John Boyle	JX 2 see Tr. 6:15-16			CX0704
RX486-A	PUBLIC Deposition Transcript of John Boyle	See OALJ Order dated 7/15/2015			CX0704-
RX487	Deposition Transcript of Brandon Bradley	JX 2 see Tr. 6:15-16			CX0705

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX487-A	PUBLIC Deposition Transcript of Brandon Bradley	See OALJ Order dated 7/15/2015			CX0705-
RX488	Deposition Transcript of Sandra Brown	JX 2 see Tr. 6:15-16			CX0706
RX489	Deposition Transcript of Matt Bureau	JX 2 see Tr. 6:15-16			CX0707
RX490	Deposition Transcript of Lou Carmicheal	JX 2 see Tr. 6:15-16			CX0708
RX491	Deposition Transcript of Mike Daugherty	JX 2 see Tr. 6:15-16			CX0709
RX492	Deposition Transcript of LabMD designee, Mike Daugherty	JX 2 see Tr. 6:15-16			CX0710
RX492-A	PUBLIC Deposition Transcript of LabMD designee, Mike Daugherty	See OALJ Order dated 7/15/2015			CX0710-
RX493	Deposition Transcript of Jeremy Dooley	JX 2 see Tr. 6:15-16			CX0711
RX494	Deposition Transcript of Erick Garcia	JX 2 see Tr. 6:15-16			CX0712
RX495	Deposition Transcript of Kim Gardner	JX 2 see Tr. 6:15-16			CX0713
RX495-A	PUBLIC Deposition Transcript of Kim Gardner	See OALJ Order dated 7/15/2015			CX0713-
RX496	Deposition Transcript of [former LabMD employee]	JX 2 see Tr. 6:15-16			CX0714
RX496-A	PUBLIC Deposition Transcript of [former LabMD employee]	See OALJ Order dated 7/15/2015			CX0714-
RX497	Deposition Transcript of Patricia Gilbreth	JX 2 see Tr. 6:15-16			CX0715
RX497-A	PUBLIC Deposition Transcript of Patricia Gilbreth	See OALJ Order dated 7/15/2015			CX0715-
RX498	Deposition Transcript of Nicotra Harris	JX 2 see Tr. 6:15-16			CX0716
RX499	Deposition Transcript of Patrick Howard	JX 2 see Tr. 6:15-16			CX0717
RX500	Deposition Transcript of Lawrence Hudson	JX 2 see Tr. 6:15-16			CX0718
RX501	Deposition Transcript of Robert Hyer	JX 2 see Tr. 6:15-16			CX0719
RX502	Deposition Transcript of Karina Jestes	JX 2 see Tr. 6:15-16			CX0720
RX503	Deposition Transcript of Eric Johnson	JX 2 see Tr. 6:15-16			CX0721
RX504	Deposition Transcript of Eric Knox	JX 2 see Tr. 6:15-16			CX0722
RX505	Deposition Transcript of David Lapides	JX 2 see Tr. 6:15-16			CX0723

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX505-A	PUBLIC Deposition Transcript of David Lapides	See OALJ Order dated 7/15/2015			CX0723-
RX506	Deposition Transcript of Chris Maire	JX 2 see Tr. 6:15-16			CX0724
RX507	Deposition Transcript of Jeff Martin	JX 2 see Tr. 6:15-16			CX0725
RX507-A	PUBLIC Deposition Transcript of Jeff Martin	See OALJ Order dated 7/15/2015			CX0725-
RX508	Deposition Transcript of Alison Simmons	JX 2 see Tr. 6:15-16			CX0730
RX509	Deposition Transcript of Alison Simmons	JX 2 see Tr. 6:15-16			CX0734
RX510	Deposition Transcript of Curt Kaloustian	JX 2 see Tr. 6:15-16			CX0735
RX511	Deposition Transcript of Jennifer Parr	JX 2 see Tr. 6:15-16			CX0727
RX511-A	PUBLIC Deposition Transcript of Jennifer Parr	See OALJ Order dated 7/15/2015			CX0727-
RX512	Deposition Transcript of Kevin Wilmer	JX 2 see Tr. 6:15-16			CX0732
RX512-A	PUBLIC Deposition Transcript of Kevin Wilmer	JX 2 see Tr. 6:15-16			CX0732-
RX513	Deposition Transcript of LeTonya Randolph	JX 2 see Tr. 6:15-16			CX0728
RX514	Deposition Transcript of Peter Sandrev	JX 2 see Tr. 6:15-16			CX0729
RX515	Deposition Transcript of Ruth Yodaiken	JX 2 see Tr. 6:15-16			
RX516	Deposition Transcript of Randall Jerry Maxey	JX 2 see Tr. 6:15-16			CX0726
RX517	Deposition Transcript of Christopher Gormley	JX 2 see Tr. 6:15-16			CX0872
RX518	Complaint Counsel's Responses to LabMD's First Set of Interrogatories	JX 2 see Tr. 6:15-16			
RX519	Complaint Counsel's Responses to LabMD's Second Set of Interrogatories	JX 2 see Tr. 6:15-16			
RX521	RX3 Yodaiken deposition	JX 2 see Tr. 6:15-16			
RX522	Deposition Transcript of Rick Kam	JX 2 see Tr. 6:15-16			
RX523	Deposition Transcript of James Van Dyke	JX 2 see Tr. 6:15-16			
RX524	Deposition Transcript of Raquel Hill	JX 2 see Tr. 6:15-16			
RX525	Deposition Transcript of Daniel Kaufman	JX 2 see Tr. 6:15-16			
RX526	Complaint Counsel's Amended Responses to LabMD's First Set of Request for Admissions	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX E CR REFE
RX527	Deposition Transcript of Karina Jestes II	JX 2 see Tr. 6:15-16			
RX528	Ponemon Survey Report	Tr. 484:19; May 18, 2015 JX0002 Joint Status Report on Exhibits	Kam, Tr. 484-489; 496; 529-531; 533-543; 554; 561-568		
RX529	Javelin Questionairre questions	Tr. 708:13; May 18, 2015 JX0002 Joint Status Report on Exhibits	Van Dyke, Tr. 701-715; 717-734		
RX532	Kaufman Deposition Transcript II	Tr. 1116:03-04; May 18, 2015 JX0002 Joint Status Report on Exhibits	Kaufman, Tr. 1115-1116		
RX533	Adam Fisk Expert Report	Tr. 1135:12-13; May 18, 2015 JX0002 Joint Status Report on Exhibits	Fisk, Tr. 1134-1175; 1179-1195; 1196; 1208; 1210; 1474		
RX541	Deposition Transcript of Robert Boback	See OALJ Order dated 7/1/2014	Tr. 1307		
RX542	June 11, 2014 OGR Letter from Issa to Ramirez	See OALJ Order dated 2/12/2015			
RX543	December 1, 2014 OGR Letter from Issa to Ramirez	See OALJ Order dated 2/12/2015			
RX545	CIGNA - Tiversa Incident Record Form ID #CIG00081	Admitted during Hearing on 5/5/2015 at 1419:6	Wallace, Tr. 1391-1396; 1400; 1411-1419; 1449-1452		
RX546	Tiversa Forensic Investigation Report August 12, 2008 for Ticket #CIG00081	Admitted during Hearing on 5/5/2015 at 1425:25	Wallace, Tr. 1398-1408; 1411-1412; 1417-1422; 1425-1426		
RX549	1718 Insurance Aging File Cover Sheet dated 6/5/07 with Wallace 00000100	Admitted during Hearing on 5/5/2015 at 1423:20	Wallace, Tr. 1409-1412; 1422-1423		
RX644	OGR Committee Report on "Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?"	See OALJ Order dated 7/15/2015			
RX645	LabMD Patient Forms/ LabMD Employee Handbook/Auditing guidelines/Insurance Documents and Payment information	See OALJ Order dated 6/22/2015	Tr. 1474-1475		
RX646	RX-15 exhibit to the Yodaiken deposition	See OALJ Order dated 6/22/2015	Tr. 1475-1476		
RX650	Nondisclosure Motion in ND GA Gormley RX-2	See OALJ Order dated 6/22/2015	Tr. 1475-1476		
RX652	Confidentiality Agreement Tiversa / Johnson RX-9	See OALJ Order dated 6/22/2015	Tr. 1475-1476		

PUBLIC

RX657	Sales Rep. Agreement (RX-1 Hudson)	See OALJ Order dated 6/22/2015	Tr. 1475-1476		

ATTACHMENT 2

IN THE MATTER OF
LABMD, INC
DOCKET NO. 9357

RESPONDENT COUNSEL'S WITNESS INDEX

NAME	BRIEF IDENTIFICATION	TRANSCRIPT REFERENCES	*IN CAMERA* STATUS
Eric Johnson	Dean of the Business School, Vanderbilt University; Former Director, Tuck Center for Digital Strategies at Dartmouth College	Tr. 749-806	Not *In Camera*
Michael Daugherty	Founder and CEO, LabMD	Tr. 936-1099	Not *In Camera*
Daniel Kaufman	Deputy Director, FTC Bureau of Consumer Protection	Tr. 1100-1117	Not *In Camera*
Adam Fisk	President and CEO, Brave New Software Project	Tr. 1123-1215	Not *In Camera*
Richard Wallace	Forensic Analyst, Tiversa	Tr. 1261-1307; 1320-1467	Not *In Camera*

Notice of Electronic Service

I hereby certify that on August 11, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Proposed Findings of Fact, with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on August 11, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Proposed Findings of Fact, upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org
Respondent

Prashant Khetan
Senior Counsel
Cause of Action
prashant.khetan@causeofaction.org
Respondent

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Patrick Massari
Attorney

EXHIBIT 31

CONFIDENTIAL — REDACTED IN ENTIRETY

EXHIBIT 32

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	PUBLIC
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

COMPLAINT COUNSEL'S AMENDED RESPONSE TO LABMD, INC.'S FIRST SET OF REQUESTS FOR ADMISSION (NUMBERS 1-20)

Pursuant to Sections 3.31 and 3.32 of the Federal Trade Commission's Rules of Practice for Adjudicative Proceedings ("Rules of Practice"), Complaint Counsel hereby amends its responses to Respondent LabMD, Inc.'s First Set of Requests for Admission ("Respondent's Requests").

Complaint Counsel has not completed its discovery or its preparation for trial. Complaint Counsel's answers to Respondent's Requests are given without prejudice to Complaint Counsel's right to produce information relating to any subsequently discovered facts. Complaint Counsel reserves the right to assert additional objections to Respondent's Requests, and to amend or supplement these objections and responses as necessary after the close of discovery.

General Objections

The following General Objections apply to each of Respondent's Requests and are hereby incorporated by reference into each response. The assertion of the same, similar, or additional objections or the provision of partial answers in response to an individual Request does not waive any of Complaint Counsel's General Objections as to the other Requests.

PUBLIC

1. Complaint Counsel objects to Respondent's definition of "Commission" and "FTC" as overly broad. The "Federal Trade Commission" (or "FTC") can act only by a majority vote of a quorum of the five Commissioners. Therefore, Complaint Counsel cannot answer these Requests on behalf of the "Federal Trade Commission" or any individual Commissioner or employee. The objections and responses to these requests are submitted on behalf of Complaint Counsel in this matter, and not on behalf of the "Federal Trade Commission," its employees, staff, agents, or attorneys other than Complaint Counsel.
2. Complaint Counsel objects to Respondent's Requests to the extent the Requests seek documents or information protected from disclosure by the attorney-client privilege, the work product doctrine, the government deliberative process privilege, the government informer privilege, the law enforcement evidentiary or investigatory privilege, common interest privilege, or any other applicable privilege or immunity. Complaint Counsel does not, by any response to any Request, waive or partially waive any applicable privilege or immunity.
3. Complaint Counsel objects to Respondent's Requests to the extent that they are not reasonably calculated to yield information relevant to the allegations of the Complaint, to the proposed relief, or to the affirmative defenses of Respondent. By responding to Respondent's Requests, Complaint Counsel does not waive or intend to waive, but rather reserves and intends to reserve: (a) any objections to the competency, relevance, materiality, privilege, or admissibility as evidence, for any purpose, of any information produced in response to Respondent's Requests; (b) the right to object on any ground to the use of information produced in response to Respondent's Requests at any hearing or trial; and (c) the right to object on any ground at any time to a demand for a further answer to Respondent's Requests.

PUBLIC

4. Complaint Counsel objects to Respondent's Requests to the extent they are overly broad, vague, ambiguous, or unduly burdensome.
5. Complaint Counsel objects to Respondent's Requests to the extent they seek information or admissions that are beyond the scope of permissible discovery under Rule 3.31(c) of the Rules of Practice. Complaint Counsel is limiting its responses to the scope of discovery set forth in Rule 3.31(c).
6. Complaint Counsel objects to Respondent's Requests to the extent they seek information that relates to expert testimony prior to the dates prescribed by the October 22, 2013 Revised Scheduling Order.
7. Complaint Counsel objects to Respondent's Requests to the extent they seek to require Complaint Counsel to admit any Request based on information that is not within Complaint Counsel's possession, custody, or control.
8. Complaint Counsel objects to Respondent's Requests to the extent that, as framed, they purport to obligate Complaint Counsel to conduct an extensive and complete investigation of detailed facts for its responses and objections when such facts are known to Respondent and/or contained in the more than 15,000 pages of documents already produced by Respondent.
9. Complaint Counsel objects to Respondent's Requests to the extent that they require Complaint Counsel to undertake legal research for Respondent.
10. Complaint Counsel objects to Respondent's Requests to the extent that they require Complaint Counsel to analyze or organize information for Respondent.
11. The failure of Complaint Counsel to object to any Request on a particular ground may not be construed as a waiver of its right to object on any additional ground(s).

PUBLIC

12. Complaint Counsel asserts that any admission contained in this response is for the purpose of the pending administrative proceeding only and is not an admission for any other purpose, nor may it be used in any other proceeding.

Each of the above-listed General Objections is incorporated by reference to each specific response and objection set forth below. Subject to and without waiving these objections, Complaint Counsel provides the following responses.

Specific Responses and Objections

Request for Admission No. 1

Admit that between 2005 and the present the FTC has not prescribed any rules or promulgated regulations regarding data-security, data security practices or data security standards for Protected Health Information ("PHI") pursuant to its authority under 15 U.S.C. § 57a(a).

Response to Request for Admission No. 1

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third and Fifth Defenses are no longer relevant to this administrative proceeding.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 1.

Request for Admission No. 2

Admit that between 2005 and the present the FTC has not prescribed any rules or promulgated regulations regarding data-security, data security practices or data security

PUBLIC

standards for PHI that defines what acts are prohibited or required under Section 5 of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45 as related to PHI.

Response to Request for Admission No. 2

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third and Fifth Defenses are no longer relevant to this administrative proceeding.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 2.

Request for Admission No. 3

Admit that the FTC does not issue advisory opinions regarding data-security practices the FTC believes to be forbidden or required by Section 5 of the FTC Act, 15 U.S.C. § 45.

Response to Request for Admission No. 3

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "advisory opinions," "forbidden," and "required." For purposes of this response, Complaint Counsel understands the term "advisory opinions" to refer to advice or interpretation provided pursuant to Sections 1.1 through 1.4 of the Rules of Practice.

PUBLIC

Complaint Counsel denies Request for Admission No. 3 to the extent that it suggests that "advisory opinions" are the only means the FTC uses to provide guidance regarding data security practices.

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel otherwise admits Request for Admission No. 3.

Request for Admission No. 4

Admit that the FTC has not accused LabMD of committing a "deceptive act or practice" under Section 5 of the FTC Act, 15 U.S.C. § 45.

Response to Request for Admission No. 4

Complaint Counsel objects to this Request to the extent it seeks to foreclose, limit, or preclude any cause of action. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits that its Complaint does not allege that Respondent committed a "deceptive act or practice" in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Request for Admission No. 5

Admit that the FTC's Complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5 of the FTC Act, 15 U.S.C. § 45.

PUBLIC

Response to Request for Admission No. 5

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. *See* Order Denying Respondent LabMD's Motion to Dismiss at 14, *In the Matter of LabMD, Inc.*, Docket No. 9357 (Jan. 16, 2014) ("information security is an ongoing process of assessing risk and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve.") (citation omitted). Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "industry standards."

Complaint Counsel denies the Request to the extent that it suggests that Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), requires Complaint Counsel to allege the specific industry standards Respondent failed to meet or specific hardware or software Respondent failed to use.

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel otherwise admits Request for Admission No. 5.

Request for Admission No. 6

Admit that the FTC has no evidence to dispute that LabMD has never been accused of violating either the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH) or any regulations implementing those statutes, including but not limited to as 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000) (HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013) (HHS HITECH rule).

PUBLIC

Response to Request for Admission No. 6

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request to the extent it seeks information protected from disclosure by the common interest, deliberative process, law enforcement, and work product privileges. Complaint Counsel further objects to this Request to the extent it seeks information outside its possession, custody or control. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Request for Admission No. 7

Admit that the FTC has not accused LabMD of violating any rules or regulations not specif.cally referenced within the four comers of the FTC's Complaint.

Response to Request for Admission No. 7

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "accused."

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 7.

PUBLIC

Request for Admission No. 8

Admit that HIPAA, HITECH, and regulations implementing those statutes are not mentioned in the FTC's Complaint.

Response to Request for Admission No. 8

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Following the Commission's January 16, 2014 Order Denying Respondent LabMD's Motion to Dismiss, Respondent's Third Defense is no longer relevant to this administrative proceeding.

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 8.

Request for Admission No. 9

Admit that the information contained in the "Day Sheets" and "P2P insurance aging file" referred to in paragraphs 20 and 21 of the Complaint constitute Protected Health Information (PHI), as that term is used in HIPAA, HITECH, and regulations implementing those statutes.

Response to Request for Admission No. 9

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request to the extent it seeks a legal conclusion regarding the application of HIPAA, HITECH and the regulations implementing those statutes.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits that the information contained

PUBLIC

in the "Day Sheets" and the "P2P insurance aging file" includes personal information, as defined in Respondent's Requests, and PHI.

Request for Admission No. 10

Admit that the FTC's consent orders are only legally binding upon the parties thereto.

Response to Request for Admission No. 10

Complaint Counsel objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "consent orders" and "legally binding."

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel denies Request for Admission No. 10.

Request for Admission No. 11

Admit that the SANS Institute does not have lawful authority to create enforceable data-security standards.

Response to Request for Admission No. 11

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "data-security standards," "lawful authority," and "enforceable."

Complaint Counsel denies Request for Admission No. 11 to the extent that it suggests that the "SANS Institute" is the only entity that provides guidance regarding data security practices.

PUBLIC

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel otherwise admits Request for Admission No. 11.

Request for Admission No. 12

Admit that the FTC did not allege that a person's data-security practices may constitute an "unfair act or practice" that violates Section 5 of the FTC Act, 15 U.S.C. § 45, until after Congress last amended Section 5 to add 15 U.S.C. § 45(n) in 1994.

Response to Request for Admission No. 12

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice.

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 12.

Request for Admission No. 13

Admit that the FTC's "Guides for Business" relating to data security, including but not limited to the FTC document entitled "Peer-to-Peer File Sharing: A Guide for Business" and "Protecting Personal Information: A Guide to Business," are not legally binding upon any U.S. company.

Response to Request for Admission No. 13

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "legally binding."

PUBLIC

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 13.

Request for Admission No. 14

Admit that none of the documents available on the Internet on the FTC's "Bureau of Consumer Protection Business Center's" self-described "Legal Resources" website, http://business.ftc.gov/legal-resources/all/35, including but not limited to consent orders and FTC "Guides for Business," establish specific data-security practices which any U.S. company must adopt to comply with 15 U.S.C. § 45(a), (n).

Response to Request for Admission No. 14

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. Complaint Counsel further objects to the form of this Request. Complaint Counsel further objects to this Request as overly broad. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "consent orders" and "adopt."

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel denies Request for Admission No. 14. A party subject to an order must comply with the specific requirements set forth in that order.

Request for Admission No. 15

Admit that the FTC has no complaining witness who says that his or her data was released or disclosed as the result of LabMD's allegedly unlawful data-security practices.

PUBLIC

Response to Request for Admission No. 15

Complaint Counsel objects to this Request to the extent that it seeks the identity and opinions rendered by non-testifying experts and seeks prematurely the opinions of expert witness(es). Complaint Counsel further objects that this Request calls for expert opinions and is not an appropriate subject for this manner of discovery. Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "released" and "disclosed."

Complaint Counsel denies Request for Admission No. 15 to the extent that it suggests that no consumers were harmed or likely to be harmed as a result of Respondent's unfair acts or practices.

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 15.

Request for Admission No. 16

Admit that Complaint Counsel was aware of the trailer to Mr. Michael Daugherty's book, The Devil Inside the Beltway, available at websitehttp://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/, prior to July 23, 2013.

Response to Request for Admission No. 16

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice. The suggestion that the FTC retaliated against Respondent in response to Respondent's speech is not relevant to this administrative proceeding. *See* Order Denying Respondent's Motion for a 3.36 Subpoena at 6, *In the Matter of*

PUBLIC

LabMD, Inc., Docket No. 9357 (Feb. 21, 2014) ("Documents that may be reasonably expected to show whether or not 'the FTC violated Daugherty's First Amendment rights by retaliating against LabMD' in fding this Complaint are not relevant to the allegations of the Complaint, the proposed relief, or the defenses of Respondent."). Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "aware."

Request for Admission No. 17

Admit that a FTC document entitled "Peer-To-Peer File Sharing: A Guide For Business," available at http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business, was not made publicly available on the Internet or otherwise published until January 2010.

Response to Request for Admission No. 17

Complaint Counsel objects to this Request as seeking an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside the scope of discovery pursuant to Section 3.31(c) of the Rules of Practice.

Subject to and without waiving the foregoing objection and General Objections, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 17.

Request for Admission No. 18

Admit that Complaint Counsel has no evidence to dispute that LabMD's "Day Sheets," which are referenced in paragraph 21 of the Complaint, did not exist in an electronic form that could be transmitted via the Internet in October 2012.

Response to Request for Admission No. 18

Complaint Counsel objects to this Request as premature because discovery and trial preparation are not complete. Complaint Counsel further objects to this Request to the extent is requires an extensive and complete investigation of all the evidence in this administrative

PUBLIC

proceeding. Complaint Counsel further objects that the Request requires Complaint Counsel to analyze the evidence for Respondents.

Subject to and without waiving the foregoing objections and General Objections, and to the extent further response is required, Complaint Counsel, after reasonable inquiry, lacks sufficient information to admit or deny Request for Admission No. 18. LabMD's "Day Sheets" were in the possession of identity thieves in Sacramento, CA on October 5, 2012, and, prior to October 5, 2012, they were transferred from LabMD's possession into the identity thieves' possession. Complaint Counsel has not yet established how the "Day Sheets" were transferred from LabMD's possession to the identity thieves' possession. LabMD implemented a data archive project to save paper documents in an electronic format. The "Day Sheets" may have been saved in an electronic form that could have been transmitted via the Internet.

Request for Admission No. 19

Admit that the FTC cannot identify a single person it believes to be a "consumer" within the meaning of the Section 5 of the FTC Act who has experienced harm to their identity or finances as a result of LabMD's allegedly unlawful data-security practices.

Response to Request for Admission No. 19

Complaint Counsel objects to this Request to the extent that it seeks the identity and opinions rendered by non-testifying experts and seeks prematurely the opinions of expert witness(es). Complaint Counsel further objects that this Request calls for expert opinions and is not an appropriate subject for this manner of discovery.

Complaint Counsel denies Request for Admission No. 19 to the extent that it suggests that no consumers were harmed or likely to be harmed as a result of Respondent's unfair acts or practices.

PUBLIC

Subject to and without waiving the foregoing objections, General Objections, and denial, and to the extent further response is required, Complaint Counsel admits Request for Admission No. 19.

Request for Admission No. 20

Admit that the FTC obtained the 1,718 File from Tiversa, Inc.

Response to Request for Admission No. 20

Complaint Counsel objects to Respondent's definition ofthe "1,718 File." Respondent defines the "1,718 File" to mean "the 1,718 page file owned by LabMD that the Company claimed in 2008 to have obtained from LabMD via Limewire." The definition of the "1,718 File" is vague and ambiguous as to "Company," "obtained," and "claimed." Complaint Counsel further objects to Respondent's characterization that the "1,718 File" was "obtained" from LabMD. The evidence in this administrative proceeding does not support this characterization. For purposes of this response, Complaint Counsel understands the term "1,718 File" to mean the 1,718 page file owned by LabMD that Tiversa Holding Corp. found at four different IP addresses. These documents have been produced by Tiversa Holding Corp. at TIVERSA-FTC_RESPONSE-000001 – 001719, TIVERSA-FTC_RESPONSE-001720 – 003438, TIVERSA-FTC_RESPONSE-003439 – 005157, and TIVERSA-FTC_RESPONSE-005158 – 006876.

Complaint Counsel further objects to this Request on the grounds that it is vague and ambiguous as to the meaning of "Tiversa, Inc." and "obtained." For purposes of this response, Complaint Counsel understands the term "Tiversa, Inc." to refer to Tiversa, as defined in Respondent's Requests.

PUBLIC

Subject to and without waiving the General Objections, and to the extent further response is required, Complaint Counsel admits that: (1) as part of Complaint Counsel's Part II investigation of LabMD, it issued a CID to the Privacy Institute and received the 1,718 file, which has been produced at FTC-PRI-000001 – FTC-PRI-001719; and (2) as part of this administrative proceeding, it issued a subpoena *duces tecum* to Tiversa Holding Corp. and received four 1,718 files downloaded from four different IP addresses. These documents have been produced at TIVERSA-FTC_RESPONSE-000001 – 001719, TIVERSA-FTC_RESPONSE-001720 – 003438, TIVERSA-FTC_RESPONSE-003439 – 005157, and TIVERSA-FTC_RESPONSE-005158 – 006876.

PUBLIC

Dated: April 1, 2014

Respectfully submitted,

Megan Cox
Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2282
Facsimile: (202) 326-3062
Electronic mail: mcox1@ftc.gov

Complaint Counsel

PUBLIC

CERTIFICATE OF SERVICE

I hereby certify that on April 1, 2014, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system.

I also certify that I caused a copy of the foregoing document to be delivered *via* electronic mail and by hand to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, NW, Room H-110
Washington, DC 20580

I further certify that I caused a copy of the foregoing document to be served *via* electronic mail to:

Michael D. Pepson
Lorinda Harris
Kent Huntington
Hallee Morgan
Robyn Burrows
Daniel Epstein
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org
lorinda.harris@causeofaction.org
kent.huntington@causeofaction.org
hallee.morgan@causeofaction.org
robyn.burrows@causeofaction.org
daniel.epstein@causeofaction.org

Reed Rubinstein
William Sherman, II
Sunni Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com
sunni.harris@dinsmore.com
Counsel for Respondent LabMD, Inc.

PUBLIC

CERTIFICATE FOR ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

April 1, 2014

By: _____

Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

EXHIBIT 33

Transcript of the Testimony of **Daniel Kaufman**

Date: May 12, 2014

Case: In The Matter of: LabMD, INC., a corporation

Ace-Federal Reporters, Inc.
Phone: 202-347-3700
Fax: 202-737-3638
Email: info@acefederal.com
Internet: www.acefederal.com

1 BEFORE THE UNITED STATES OF AMERICA
2 FEDERAL TRADE COMMISSION
3 OFFICE OF ADMINISTRATIVE LAW JUDGES
4
5 - - - - - - - - - - - - - - - x
6 In the Matter of: : Docket Number
7 LABMD, INC., a corporation, : 937
8 Respondent. :
9 - - - - - - - - - - - - - - - x
10
11
12 DEPOSITION OF DANIEL KAUFMAN, VOLUME II
13
14
15 Washington, D.C.
16 Monday, May 12, 2014
17
18
19
20 REPORTED BY:
21 SARA A. WICK, RPR, CRR
22

1 Volume II deposition of DANIEL KAUFMAN, called
2 for further examination pursuant to notice of
3 deposition on Monday, May 12, 2014, in Washington,
4 D.C., at the offices of the Federal Trade
5 Commission, 600 Pennsylvania Avenue Northwest, Room
6 722G, at 9:39 a.m., before SARA A. WICK, RPR, CRR,
7 and a Notary Public within and for the District of
8 Columbia, when were present on behalf of the
9 respective parties:
10
11 LAURA RIPOSO VAN DRUFF, ESQ.
12 Federal Trade Commission
13 Division of Privacy and Identity Protection
14 600 Pennsylvania Avenue Northwest
15 Mail Stop NJ-8100
16 Washington, D.C. 20580
17 202-326-2999
18 lvandruff@ftc.gov
19 On behalf of the Federal Trade Commission
20
21 -- continued --
22

1 APPEARANCES (continued):
2
3 WILLIAM SHERMAN, II, ESQ.
4 Dinsmore & Shohl LLP
5 801 Pennsylvania Avenue Northwest
6 Suite 610
7 Washington, D.C. 20004
8 202-372-9117
9 william.sherman@dinsmore.com
10 On behalf of Respondent
11
12 KENT HUNTINGTON, ESQ.
13 Cause of Action
14 1919 Pennsylvania Avenue Northwest
15 Suite 650
16 Washington, D.C. 20006
17 202-499-2426
18 kent.huntington@causeofaction.com
19 On behalf of Respondent
20
21
22

1 P R O C E E D I N G S
2 (Exhibit Kaufman 1 identified.)
3 Whereupon,
4 DANIEL KAUFMAN,
5 was recalled as a witness and, having first been
6 duly sworn, was examined and testified further as
7 follows:
8 EXAMINATION
9 BY MR. SHERMAN:
10 Q Good morning, Mr. Kaufman.
11 A Good morning.
12 Q It's your understanding and at least it's
13 my understanding that this is a continuation of the
14 deposition that we had begun earlier, and I had
15 asked you certain questions about data security and
16 data security standards. Your counsel objected. We
17 filed a motion.
18 And what I've handed you marked as RX-1
19 for purposes of this deposition is the order
20 granting Respondent's motion to compel testimony.
21 Have you seen that document before?
22 A No, I have not.

1 Q Okay. I will submit to you that this
2 order is the reason why we're here today. As I
3 previously explained in the prior deposition, your
4 counsel had objected to a certain line of
5 questioning regarding data security, and the Court
6 has since that time ruled that we do have the right
7 to question you with regard to data security.
8 Are you prepared today to testify with
9 regard to data security standards that the Bureau or
10 the FTC plans to use to support its allegations
11 against LabMD?
12 A Yes, I am.
13 (Exhibit Kaufman 2 identified.)
14 BY MR. SHERMAN:
15 Q Mr. Kaufman, I've just handed you what's
16 been marked for identification purposes for this
17 deposition a document that's labeled RX-2, and it's
18 entitled the "Complaint."
19 Have you seen the complaint that was filed
20 in this matter before?
21 A Yes.
22 Q I would ask that you turn to paragraph

1 10(a) of the complaint, which can be found on page
2 3. Paragraph 10 reads that "At all relevant times,
3 Respondent engaged in a number of practices that,
4 taken together, failed to provide reasonable and
5 appropriate security for personal information on its
6 computer networks. Among other things, Respondent,"
7 and it goes into subparagraphs.
8 Subparagraph (a) says that "Respondent did
9 not develop, implement, or maintain a comprehensive
10 information security program to protect consumers'
11 personal information."
12 Did I read that correctly?
13 A Yes.
14 Q Is it the Bureau's position that in order
15 to comply with or to avoid violation of Section 5 of
16 the Federal Trade Commission Act as it relates to
17 data security, an entity must have in place a
18 comprehensive information security program?
19 A Are we talking about a deception
20 allegation or an unfairness allegation?
21 Q It's my understanding, and you correct me
22 if I'm wrong, that the Bureau has accused LabMD of

1 an unfair practice and that the Bureau has not
2 alleged that LabMD has committed any deception.
3 Is that your understanding?
4 A That is my understanding.
5 Q Okay. Then my questions will be limited
6 to unfair practices as it relates to the allegations
7 against LabMD.
8 And so my question, then, in that regard
9 is, is it the Bureau's position that in order to
10 comply with Section 5 of the Federal Trade
11 Commission Act, that an entity must have in place a
12 comprehensive information security program?
13 A Assessing whether certain data security
14 practices are unfair under Section 5 of the FTC Act
15 requires a case-by-case factual analysis of the
16 situation. So whether a company has developed,
17 implemented, or maintained a comprehensive
18 information security program may be required under
19 Section 5.
20 Q Is it the Bureau's position that, based on
21 its analysis of the facts in this case, that it will
22 hold LabMD to the standard of requiring a

1 comprehensive information security plan?
2 MS. VAN DRUFF: I'm sorry. May I ask that
3 that question be repeated.
4 (Record read by the court reporter as
5 requested.)
6 MS. VAN DRUFF: And counsel, just for
7 purposes of clarification, are you asking for an
8 explanation of paragraph 10(a), or are you asking
9 Mr. Kaufman whether 10(a) says what it says?
10 MR. SHERMAN: I think we know what it
11 says. I'm not asking him to explain what it says.
12 I'm asking him a very direct question --
13 THE WITNESS: Uh-huh.
14 MR. SHERMAN: -- of whether or not, based
15 on the analysis, case-by-case analysis in this
16 particular case, whether the Bureau's position is
17 that it will hold LabMD to the standard of having to
18 have a comprehensive information security program in
19 order to comply with Section 5.
20 THE WITNESS: The Bureau will allege that
21 one of LabMD's failings, among others, was the
22 failure to have a comprehensive information security

1 program.
2 BY MR. SHERMAN:
3 Q Has the Bureau published or otherwise
4 informed the public that HIPAA-covered entities such
5 as LabMD must have a written comprehensive
6 information security program in place in order to
7 comply with FTC or Bureau data security standards?
8 A I am not sure whether the Commission has
9 issued material specifically relating to the
10 HIPAA-covered entities, but the Bureau has published
11 a great deal of consumer and business education on
12 the issue of what is reasonable data security.
13 The Commission has testified on it on a
14 number of occasions, and there's a lot of other
15 publicly available information on what constitutes
16 reasonable data security.
17 Q Is it the Bureau's position that
18 reasonable data security, as it has analyzed this
19 case, as it does on a case-by-case basis, includes
20 having in place a comprehensive information security
21 plan?
22 MS. VAN DRUFF: And counsel, are you

1 asking -- sorry, that sounded like two questions,
2 generally and as it relates to this case. Which is
3 the question?
4 MR. SHERMAN: As it relates to this case.
5 THE WITNESS: Okay. Can I hear that back.
6 (Record read by the court reporter as
7 requested.)
8 THE WITNESS: In this case the Bureau has
9 alleged that LabMD should have had a comprehensive
10 information security program in place.
11 BY MR. SHERMAN:
12 Q Is the Bureau's definition of a
13 comprehensive information security program the same
14 as the definition for a comprehensive information
15 security program as set out in Dr. Raquel Hill's
16 expert witness report?
17 A I am not aware of a specific definition we
18 have used for comprehensive information security
19 program, but I can certainly look at her definition
20 and see if it seems consistent with my general
21 understanding.
22 Q That's the only reason I brought it.

1 A Okay.
2 (Exhibit Kaufman 3 identified.)
3 BY MR. SHERMAN:
4 Q Mr. Kaufman, you've been handed what's
5 been marked as RX-3 for identification purposes for
6 this deposition. I submit to you that it is a copy
7 of the expert witness report of Dr. Raquel Hill,
8 without the exhibits that were attached to the
9 original report.
10 Have you seen this report before?
11 A Yes.
12 Q I'm going to ask you to turn to page 19 of
13 the report and to look at paragraph 52. Paragraph
14 52 reads "A comprehensive information security
15 program is a plan that sets out an organization's
16 security goals, the written policies that would
17 satisfy those goals, the mechanisms that would be
18 used to enforce the written policies, and how those
19 mechanisms would be used to enforce the written
20 policies."
21 Did I read that correctly?
22 A Yes.

1 Q Is that the Bureau's definition of
2 a comprehensive information security program?
3 A I am not aware of the Commission having a
4 definition for a comprehensive information security
5 program. I know we have stated in business
6 education materials generally what a comprehensive
7 information security program would require.
8 But what is written here in Professor
9 Hill's report appears consistent with what we have
10 said in the past. I think it's as a matter of
11 semantics or different words that are probably being
12 used here. But at its core, it seems quite
13 consistent.
14 Q Paragraph 52 goes on to say that "The best
15 practices for developing a comprehensive information
16 security program would include the seven principles
17 that I," Dr. Hill referring to herself, "discuss in
18 paragraph 31, above: Don't keep what you don't
19 need, patch, ports, policies, protect, probe, and
20 physical."
21 Did I read that correctly?
22 A Yes.

1 Q Does the Bureau adhere to the notion that
2 the best practices for developing a comprehensive
3 information security program includes the seven
4 principles set out in Dr. Hill's report?
5 A I think the best practices for developing
6 a comprehensive information security program is
7 going to be fairly case specific, but the principles
8 that she lays out here are, again, consistent with
9 my understanding of what those best practices would
10 be.
11 Q Has the Bureau published any information
12 which would indicate to HIPAA-covered entities like
13 LabMD that they are expected to apply the seven
14 principles of best practices as it relates to a
15 comprehensive information security program as
16 explained in Dr. Hill's report?
17 A The Bureau has published a great deal of
18 materials that provide guidance regarding
19 comprehensive information security programs from the
20 50 or so settlement orders that have been issued by
21 the FTC that provide such information to business
22 educational, to speeches, to Congressional

1 testimony, and there's additional information
2 available from other organizations as well.
3 Q In any of that literature or the documents
4 that you referenced, is the phrase "comprehensive
5 information security program" used?
6 A I'm not sure.
7 Q In any of the information that you just
8 referenced, do they contain the seven principles as
9 stated in Dr. Hill's report with regard to best
10 practices to establish a comprehensive security --
11 I'm sorry, a comprehensive information security
12 program and list those seven principles as don't
13 keep what you don't need, patch, ports, policies,
14 protect, probe, and physical?
15 A The concepts that are set forth by the
16 seven principles are very consistent with other
17 information that I have seen in some of our
18 materials, including our business educational
19 materials.
20 Q And when you are referencing the business
21 education materials, when did the FTC start
22 publishing business education materials as it

1 relates specifically to data security?
2 A My understanding is that the earliest
3 business educational materials are from 2003.
4 Q And has the FTC or the Bureau continued to
5 publish business education materials related to data
6 security from that time through the present?
7 A Yes, we've done both written materials and
8 videos.
9 Q You mentioned 50 decisions, and I may be
10 using the wrong word because I forgot what --
11 A I said settlements.
12 Q 50 settlements. In any of those
13 settlements, to your knowledge, is the phrase
14 "comprehensive information security program" used?
15 A I would have to take a look. It would not
16 surprise me if they were; it wouldn't surprise me if
17 there was a similar term that was used. The concept
18 is embedded within those orders. But again, I don't
19 have the stack of 50 in front of me, but they're
20 available on our Web site at ftc.gov.
21 Q So is it your -- is it the Bureau's
22 position that in order to discern or discover what

1 data security requirements the Bureau or the FTC
2 expects business entities to comply with with regard
3 to data security can be found on the FTC Web site?
4 A Can I hear that again?
5 MS. VAN DRUFF: Objection; misstates prior
6 testimony.
7 If you could repeat the question, please.
8 (Record read by the court reporter as
9 requested.)
10 THE WITNESS: The Commission has
11 consistently applied the unfairness test in
12 assessing the adequacy of data security. A great
13 deal of information about that is on the Web site.
14 A great deal of information is also available from
15 other sources.
16 BY MR. SHERMAN:
17 Q Has the Bureau or the FTC informed
18 business entities that it should consult the FTC's
19 Web site in order to discern what the Bureau or the
20 FTC's data security requirements are?
21 A Can I hear that back also.
22 (Record read by the court reporter as

1 requested.)
2 A Yes, we have. The whole purpose of doing
3 all the business education that we do is to get the
4 information out there, and we get it out through
5 whether it's speeches or media interviews or the
6 like. There's been a great deal of focus on the
7 availability of this kind of information on the
8 FTC's Web site and on other sources.
9 Q Has the FTC or the Bureau specifically
10 informed HIPAA-covered entities that they, too,
11 should refer to the FTC Web site, FTC settlements,
12 and the other information that the FTC has published
13 in order to discern what is required of them by the
14 FTC or the Bureau in order to comply with data
15 security requirements and the fairness doctrine as
16 set out in Section 5?
17 MS. VAN DRUFF: Objection; vague as to
18 "fairness doctrine" and as to "HIPAA-covered
19 entities."
20 You may answer.
21 THE WITNESS: Sure. I do not have a legal
22 opinion as to what kind of entities are subject to

1 HIPAA.
2 But that said, we very broadly reached out
3 to a wide range of businesses in terms of the
4 availability of this information on our Web site and
5 the need for reasonable data security.
6 BY MR. SHERMAN:
7 Q Is it the Bureau's position that LabMD is
8 a HIPAA-covered entity?
9 A That is a legal question, and I do not
10 have an answer for it.
11 Q So it's your testimony -- or is it your
12 testimony, because I don't want to assume, is it
13 your testimony that the Bureau or the Commission has
14 not specifically reached out to HIPAA-covered
15 entities to make them aware of what data security
16 standards would be applied to them, meaning
17 HIPAA-covered entities as it relates to what the
18 Bureau or the FTC would expect in order to comply
19 with data security standards as set out by Section 5
20 of the Act?
21 A If you're asking whether I'm aware of
22 specific material that focuses on HIPAA-covered

1 entities, I am not aware of such material.
2 But that said, all of our business
3 educational materials and other materials are highly
4 relevant to HIPAA-covered entities and other
5 entities as well.
6 Q My question is a bit more specific. Has
7 the Bureau or the Commission reached out to
8 HIPAA-covered entities in particular and made them
9 aware that there are -- that the FTC or the Bureau
10 has data security requirements outside of HIPAA
11 which they expect these entities to comply with?
12 MS. VAN DRUFF: Objection as to "outside
13 of HIPAA."
14 You may answer if you can.
15 THE WITNESS: Can you explain what you
16 mean by "reached out to"? I think that's where I'm
17 a little confused.
18 BY MR. SHERMAN:
19 Q What I'm trying to figure out is whether
20 or not the Commission or the Bureau has specifically
21 published information that would target
22 HIPAA-covered entities to make them aware that the

1 Commission and the Bureau expect certain data
2 security compliance measures to be in place.
3 A As I previously said, I am not aware of
4 any material that is specifically directed to HIPAA
5 entities. But the materials that I am aware of have
6 broad application above and beyond just general
7 non-HIPAA entities.
8 Additionally, I would find it safe to
9 assume that a number of FTC Staff and Commissioners
10 have made presentations and speeches at audiences
11 that would include HIPAA-covered entities.
12 Q You're making an assumption about that, of
13 course?
14 A Yes, yes, I am. I think it's safe to make
15 that assumption in light of the extensive outreach
16 the Commission does.
17 Q Has the FTC or the Bureau informed the
18 public, including HIPAA-covered entities such as
19 LabMD, that one of the principles of best practices
20 for a comprehensive information security plan is
21 don't keep what you don't need?
22 A Yes, that principle is clearly laid out in

1 our business educational materials.
2 Q And has the FTC and/or the Bureau made it
3 known that entities must adhere to this principle in
4 order to comply with FTC or Bureau data security
5 standards?
6 MS. VAN DRUFF: Objection; misstates prior
7 testimony.
8 You may answer.
9 THE WITNESS: That concept is one of the
10 factors that are considered. I don't think I said
11 that it must occur.
12 BY MR. SHERMAN:
13 Q I didn't say that you did.
14 A I think it's the best practice. Actually,
15 if we can read the question back.
16 Q Sure.
17 (Record read by the court reporter as
18 requested.)
19 A If I can clarify my answer, we've made it
20 clear that this is one of the practices that
21 companies should consider as they're developing data
22 security practices.

1 Q Is this one of the principles that the
2 Bureau would look at in evaluating on a case-by-case
3 basis whether or not an entity has complied with the
4 Bureau or the Commission's data security standards?
5 MS. VAN DRUFF: Mr. Sherman, I will permit
6 Mr. Kaufman to answer that question generally, but
7 as we get into specific applications, that gets into
8 the mental processes of counsel.
9 You're asking the question generally, I
10 understand; is that correct?
11 MR. SHERMAN: Yes.
12 THE WITNESS: It's one of the areas we
13 would look at in assessing whether data security
14 practices were unfair under Section 5.
15 BY MR. SHERMAN:
16 Q Is it one of the principles that the
17 Bureau would look at and consider each time that it
18 is investigating as whether or not an entity's
19 security practices were adequate?
20 A It is something that we would frequently
21 look at. Whether we've looked at it every single
22 time, I can't say, but certainly, it's commonly

1 looked at.
2 Q And so consistent with your previous
3 answers, these evaluations and considerations of
4 adherence to these principles is analyzed on a
5 case-by-case basis; is that fair to say?
6 A We review each case on a case-by-case
7 basis and do a fact-specific analysis.
8 Q And in reviewing the case on a
9 case-by-case basis, is it fair to say that the FTC
10 looks at all seven principles as laid out in
11 Dr. Hill's report?
12 MS. VAN DRUFF: Counsel, are you asking
13 Mr. Kaufman whether, in conducting the
14 reasonableness inquiry that he's described, whether
15 in every case the Bureau considers the principles
16 set forth in paragraph 52 of Dr. Hill's report?
17 MR. SHERMAN: I'm asking whether or not
18 the Bureau considers the seven principles when they
19 are evaluating a case on a case-by-case basis.
20 THE WITNESS: I don't know that the seven
21 principles are each considered on every case, but
22 generally speaking, these principles are looked at

1 on most cases.
2 BY MR. SHERMAN:
3 Q Has the --
4 A For example, there might not be a reason
5 to focus on physical in a certain case. So we might
6 not actually look at that if we're just focused on
7 electronic security.
8 Q Has the Commission or the Bureau published
9 any literature or made the public generally aware by
10 any means or any of the means that you've previously
11 mentioned that these seven principles for a
12 comprehensive information data security program will
13 be looked at in evaluating whether or not an entity
14 is in compliance with the Commission's or the
15 Bureau's data security standards?
16 A Can I hear that one more time?
17 (Record read by the court reporter as
18 requested.)
19 A That's a long question, but it is very
20 consistent with what I've seen in business education
21 materials, in speeches, in Congressional testimony,
22 and in other similar materials.

1 Q Has it been set out as principles, as the
2 seven principles of best practices for a
3 comprehensive information data security program?
4 A As I said previously, I don't believe we
5 have laid it out specifically as these seven
6 principles, but these seven principles are very
7 consistent with the principles that we have laid out
8 within our materials. These are Dr. Hill's seven
9 principles, and they are utterly consistent --
10 consistent with what the FTC or the Bureau has
11 stated.
12 Q If we will go back to the complaint, I
13 think you're still there. No, you're not. You're
14 at Dr. Hill's report. Yes, the complaint, which is
15 RX-2. Again, we're at page 3. Subparagraph (b)
16 reads "did not use readily available measures to
17 identify commonly known or reasonably foreseeable
18 security risks and vulnerabilities on its networks.
19 By not using measures such as penetration tests, for
20 example, Respondent could not adequately assess the
21 extent of the risks and vulnerabilities of its
22 networks."

1 Did I read that correctly?
2 A Yes.
3 Q Has the Commission or the Bureau published
4 information which indicates that an entity must use
5 penetration tests to identify commonly known or
6 reasonably foreseeable security risks or
7 vulnerabilities on its network?
8 A The Commission has, through all the
9 materials I've mentioned, said that companies need
10 to use readily available measures to identify
11 reasonably known security risks, and one of the
12 methods of doing that would be penetration tests.
13 Q Is the use of penetration tests a
14 requirement in order to -- in order for an entity to
15 comply with the Commission's or the Bureau's data
16 security standards?
17 A Whether or not a penetration test is
18 needed is something we would talk to a consulting
19 expert about in terms of assessing the
20 reasonableness of the data security. There might be
21 other means of identifying reasonably foreseeable
22 security risks, but penetration tests would be one

1 means of doing that.
2 Q So is it fair to say that your testimony
3 is that whether or not an entity should use
4 penetration tests is determined on a case-by-case
5 basis?
6 A Yes.
7 Q Has the Commission or the Bureau published
8 information which informed entities that the use of
9 penetration tests in order to determine and identify
10 commonly known or reasonably foreseeable security
11 risks and vulnerabilities on its networks would be
12 determined on a case-by-case basis by the Bureau or
13 the Commission?
14 A Our business education materials have made
15 it clear that one means of assessing reasonably
16 foreseeable security risks is penetration tests and
17 lays out other means as well.
18 Q In those business materials or other
19 published materials, has the Commission or the
20 Bureau informed business entities that the use of
21 penetration tests in order to secure data would be
22 determined on a case-by-case basis?

1 A We've made it clear that penetration tests
2 are one means of assessing reasonably foreseeable
3 security risks and that it's one of the tests or
4 procedures that companies should engage in in
5 developing their security plan.
6 Q Has the Commission or the Bureau informed
7 the public, business entities that deal with data
8 security that the data security requirements that
9 the Commission and the Bureau will look at in order
10 to determine whether or not that business entity is
11 in compliance with Section 5 will be done on a
12 case-by-case basis?
13 A Yes, I've seen a number of Commission
14 materials that have made it clear that we do a
15 case-by-case assessment to determine whether data
16 security practices are reasonable, from speeches, to
17 Congressional testimony, to business educational
18 materials.
19 Q Do you have a date range for when the
20 Commission or the Bureau began advising business
21 entities that these determinations would be made on
22 a case-by-case basis?

1 A I know our business educational materials
2 started as early as 2003, and I'm sure people were
3 providing speeches to business at or about that time
4 as well. But I would have to look at specific
5 documents to see, you know, what's contained in the
6 speeches or testimony or business ed or consumer ed.
7 Q So it's your belief as we sit here
8 currently that from 2003 on it's been the stated
9 policy of the Commission or the Bureau to inform
10 business entities that a determination of the data
11 security requirements as they relate to compliance
12 with Section 5 will be determined on a case-by-case
13 basis?
14 MS. VAN DRUFF: Objection; vague as
15 to "stated policy."
16 You may answer.
17 THE WITNESS: I'm not sure if I can answer
18 that. I mean, we brought our first unfairness test
19 involving data security in 2005. So prior to that,
20 the focus might have been more on the deception
21 analysis in terms of representations that companies
22 made regarding their data security.

1 And I know we've been talking primarily
2 about unfairness. So prior to 2005, I'm not quite
3 sure what the materials would have said, but
4 certainly, I've seen many materials that have made
5 it clear to business that we assess these things on
6 a case-by-case basis and that there's
7 no-one-size-fits-all data security plan.
8 BY MR. SHERMAN:
9 Q Has the Bureau or the Commission published
10 information that would inform business entities that
11 a comprehensive information security program and the
12 seven principles of best practice that apply to it
13 would be determined on a case-by-case basis?
14 MS. VAN DRUFF: Objection; vague.
15 You may answer.
16 THE WITNESS: Yes, my understanding is
17 those concepts have been laid out clearly in
18 speeches, business educational materials,
19 Congressional testimony, and through -- that's it.
20 BY MR. SHERMAN:
21 Q Let's go back to RX-2, subparagraph C,
22 which reads "did not use adequate measures to

1 prevent employees from accessing personal
2 information not needed to perform their jobs."
3 Did I read that correctly?
4 A Yes.
5 Q Has the Commission or the Bureau published
6 information to the general public and business
7 entities that in order to comply with the data
8 security standards as the Commission or the Bureau
9 sees it under Section 5, that they should use
10 adequate measures to prevent employees from
11 accessing personal information not needed to perform
12 their jobs?
13 MS. VAN DRUFF: Objection; lack of
14 foundation.
15 You may answer.
16 THE WITNESS: Yes, that is a principle
17 that I have seen in business educational materials,
18 speeches, Congressional testimony.
19 It's also certainly consistent with
20 information that's been in the 50 or so different
21 FTC -- some of the 50 or so different FTC
22 settlements involving data security matters.

1 BY MR. SHERMAN:
2 Q Has the Commission or the Bureau published
3 information that informs business entities that they
4 should review Commission settlements in order to
5 determine what the data security standards the
6 Commission or the Bureau would expect entities to
7 adhere to?
8 MS. VAN DRUFF: Objection; misstates prior
9 testimony.
10 You may answer.
11 THE WITNESS: Yes, certainly, I've seen a
12 number of speeches to industry where we discuss
13 specific cases and data security issues that were at
14 stake, and we emphasized that the complaints and
15 orders that the Commission has issued are highly
16 informative on a wide variety of areas.
17 BY MR. SHERMAN:
18 Q And do you have a time frame in which the
19 Commission or the Bureau began advising the public
20 that -- and let's talk about unfairness, since
21 that's what this case is about -- that the
22 settlements are a proper source for them to look at

1 to determine what data security standards are
2 expected of them by the Commission and/or the
3 Bureau?
4 A You know, I would have to look at specific
5 documents. But I can certainly state that I started
6 working for Chairman Majoris as one of her advisors
7 in May 2005, and I worked on a number of speeches
8 that she delivered to industry in a wide variety of
9 fora, and she would routinely discuss data security
10 matters and specific data security cases that the
11 Commission has brought.
12 Q Would she discuss the fact that looking at
13 settlements between the Commission and/or the Bureau
14 is a good source for businesses to reference when
15 they are trying to determine what data security
16 standards or expectations the Commission or the
17 Bureau would have of them?
18 A I haven't looked at her speeches in many
19 years, but it would surprise me if that concept did
20 not appear in some or many of her speeches about
21 data security.
22 I will emphasize that she always wanted us

1 to write speeches that really opined on what the
2 issues were and what industry can learn from the
3 cases. So it's utterly consistent with the speeches
4 that she would give as chairman.
5 Q Other than mentioning this process of
6 looking at settlements to determine what the
7 Commission's data security standards were, were
8 there any other -- was there any other information
9 sent out to the public informing them that looking
10 at Commission settlements was a good source for
11 determining what the Commission or the Bureau data
12 security standards were?
13 A Certainly, those are business educational
14 materials, which again I would have to look at them,
15 but I'm pretty sure that concept appears in them.
16 Additionally, there are blogs that the
17 Commission does for the business community. That
18 just started in the last few years. There's
19 Congressional testimony that we've given on the
20 point since about 2003.
21 So I think there's a wide variety of
22 materials that make that point in different

1 fashions.
2 Q Are the speeches that you referred to
3 posted on the FTC Web site?
4 A Generally, yes. I should say that
5 generally, yes, if it's a formal speech. Sometimes
6 people will do panels or the commissioners would do
7 panels where it's more Q and A, and those generally
8 are not posted, but they're often done on data
9 security issues as well. I know the speeches I
10 wrote for Former Chairman Majoris are still on the
11 Web site and have been since 2005.
12 Q What about testimony before Congress?
13 A It's all on our Web site.
14 Q How long is that information maintained on
15 the Web site?
16 A I think you can go on the Web site -- I
17 think you can go on our Web site right now and pull
18 back our testimony from as early as 2003, but I
19 would have to go online. We recently revamped the
20 Web site a few months ago, and I'm not sure every
21 link is live at the moment, but most of them are.
22 And I should say that I'm quite familiar

1 with this because I've written a lot of testimony
2 and speeches, and I routinely will pull up
3 Congressional testimony from our Web site. It's a
4 source not just for business, but for me as well.
5 Q Let's go to subparagraph (d).
6 A Could we take a break before we do that?
7 Q Absolutely.
8 A Thanks.
9 (Recess.)
10 BY MR. SHERMAN:
11 Q Before we took a break, I was about to ask
12 you about subsection (d) in paragraph 10 in terms of
13 it reads "did not adequately train employees to
14 safeguard personal information."
15 And my question, as it has been, is has
16 the Commission or the Bureau published information
17 to the general public or to entities like LabMD that
18 one of the requirements in order to comply with
19 Section 5 would be that it would need to train its
20 employees or adequately train its employees to
21 safeguard personal information?
22 A Consistent with what I've said previously,

1 the Bureau and the Commission has published a wide
2 range of materials that have explained that training
3 employees to safeguard personal information is one
4 of the things that should be done in developing
5 and -- developing a data security program.
6 Q And is training of employees something
7 that the Commission or Bureau looks at each time as
8 it's evaluating a case on a case-by-case basis?
9 A I can't say that it's something that we
10 look at each time, but I know on many occasions we
11 will look at it. And when we're -- as a part of an
12 investigation, we will get copies of a company's
13 data security programs if there are written
14 programs. And certainly, training is something we
15 would look for in those documents, as well as the
16 implementation of the program.
17 Q Let's look at subsection (e), which
18 says "did not require employees, or other users with
19 remote access to the networks, to use common
20 authentication-related security measures, such as
21 periodically changing passwords, prohibiting the use
22 of the same password across applications and

1 programs, or using two-factor authentication."
2 Did I read that correctly?
3 A Yes.
4 Q Are there materials out there that have
5 been published by the Commission or the Bureau
6 indicating that entities will be required to employ
7 authentication-related security measures,
8 periodically changing their passwords, prohibiting
9 the use of same passwords across applications, and
10 using two-factor authentication in order to comply
11 with Section 5?
12 A I know the materials I've looked at have
13 discussed the importance of good password practices.
14 Whether each of them has gone into the specificity
15 of each of the items you mentioned, I'm not sure,
16 but the general concept of changing passwords and
17 making sure they're complex and two-factor
18 authentication for remote access is certainly
19 embedded in many of those materials.
20 Q Is there published information by the
21 Commission or the Bureau which lets business
22 entities know that this type of -- these types of

1 security-related measures as listed in subparagraph
2 (e) are the type that the Commission and the Bureau
3 will look at on a case-by-case basis in order to
4 determine compliance with Section 5?
5 A Yes, through speeches, business education,
6 Congressional testimony, articles, blog entries,
7 these concepts have been laid out pretty clearly in
8 Commission materials, as well as other FTC
9 settlements in the data security area.
10 Q Subparagraph (f) reads "did not maintain
11 and update operating systems of computers and other
12 devices on its networks. For example, on some
13 computers Respondent used operating systems that
14 were unsupported by the vendor, making it unlikely
15 that the systems would be updated to address newly
16 discovered vulnerabilities."
17 Do you see that?
18 A Yeah.
19 Q Again, is there published materials out
20 there by the Commission or the Bureau which
21 indicates that these particular factors would be
22 looked at in assessing whether or not a business

1 entity is in compliance with Section 5?
2 A Certainly, I've seen this concept in our
3 business education materials, emphasizing the
4 importance of maintaining and updating operating
5 systems. That concept certainly appears in there
6 and probably in other materials as well, but
7 business ed is what jumps at me first.
8 Q In terms of subparagraph (g), "did not
9 employ readily available measures to prevent or
10 detect unauthorized access to personal information
11 on its computer networks. For example, Respondent
12 did not use appropriate measures to prevent
13 employees from installing on computers applications
14 or materials that were not needed to perform their
15 jobs or adequately maintain or review records of
16 activity on its networks."
17 Did I read that correctly?
18 A Yes.
19 Q Is there published information out there
20 from the Commission or the Bureau that capsulizes
21 these concepts as well?
22 A Sure. I'm pretty sure those concepts

1 appear in our business educational materials as
2 well.
3 Q So is it the Bureau's position that LabMD
4 could have learned of each of these requirements in
5 the subparagraphs of paragraph 10 of the complaint
6 by researching the published business literature
7 from the Commission, looking at the Commission's
8 testimony before Congress, researching speeches made
9 by commissioners, tracking the blogs of the
10 commissioner, and generally following the
11 information that was published by the Commission?
12 MS. VAN DRUFF: Objection; misstates prior
13 testimony.
14 You may answer.
15 THE WITNESS: I would say that the
16 Commission has consistently applied the three-part
17 test in assessing whether practices were unfair.
18 We've published a great deal of information
19 providing guidance and information about certain
20 data security practices, and that information has
21 been publicly available. But at its core, it is all
22 about reasonableness under Section 5.

1 BY MR. SHERMAN:
2 Q And the three-part test that you're
3 referring to is what?
4 A It is the unfairness test, which in order
5 to assess whether a practice is unfair, we have to
6 show that it causes or likely to cause
7 substantial -- causes or likely to cause substantial
8 injury that is, two, not reasonably avoidable by
9 consumers themselves and, three, that is not
10 outweighed by countervailing benefits to consumers
11 or competition.
12 Q That's better than you did the first time.
13 A Yes, much better than I did last time.
14 Thank you for pointing that out. You caught me off
15 guard last time, and my brain was not working. It
16 was painful reading that back in the transcript. I
17 wanted to correct it, but it was what I said.
18 Q I gave you the opportunity, and you did
19 well. In your testimony, we've talked about a lot
20 of different sources from which the information
21 could have been gleaned by LabMD as to what data
22 security practices or standards would have been

1 acceptable to the Commission.
2 What we have in front of us is the
3 complaint, which we've gone through each of the
4 subsections of the main allegations, I will call it,
5 but we also have Dr. Hill's expert witness report.
6 And my question is whether it's the
7 Bureau's position that LabMD should have taken each
8 action as outlined in Dr. Hill's report.
9 A I can't state that every single action
10 that's stated in her report was required. Clearly,
11 Dr. Hill has done a thorough analysis of the
12 programs or lack thereof that were in place by LabMD
13 and has had significant problems with what they did,
14 but I can't say that one in isolation would sort of,
15 per se, have been a problem. I just can't point to
16 one in particular, if that answers your question.
17 Q Is Dr. Hill's report a fair example of
18 what the Commission and the Bureau mean by each case
19 will be evaluated on a case-by-case basis?
20 MS. VAN DRUFF: Objection; vague as
21 to "fair example."
22 You may answer.

1 THE WITNESS: I would say in most of our,
2 if not all of our data security cases, we work with
3 outside experts to assess the reasonableness of the
4 practices. Obviously, the Dr. Hill report has been
5 put into writing. So it's probably different than
6 what we do in a lot of cases where it is not
7 necessarily put into writing. So it is different in
8 that sense.
9 But we will talk to experts about
10 certainly many, if not all of the issues that are
11 raised by Dr. Hill's report in other cases.
12 BY MR. SHERMAN:
13 Q Is Dr. Hill's report and the concepts and
14 principles set out therein the standard, the data
15 security standard that the Commission and/or the
16 Bureau will hold LabMD to meet?
17 A At its core, unfairness requires
18 reasonableness, and what Dr. Hill has done here is a
19 much more granular analysis of LabMD's practices
20 that apply to LabMD and the case-specific analysis
21 for LabMD. So I can't generalize what she has said
22 here to other entities.

1 Q And that's fair, and what I'm -- the
2 question was, is this the standard that will be
3 applied to LabMD. You've already testified that
4 each case will be assessed on a case-by-case basis,
5 and obviously, this is, as you stated, a granular
6 analysis of LabMD's data security practices.
7 The question is, is this the standard to
8 which the Commission believes LabMD should have had
9 its data security practices, and anything less the
10 Commission would have deemed unreasonable?
11 MS. VAN DRUFF: Counsel, by "this," are
12 you referring to Dr. Hill's report or the Section 5
13 reasonable analysis that Mr. Kaufman testified
14 about?
15 MR. SHERMAN: Dr. Hill's report.
16 THE WITNESS: The standard is Section 5
17 and reasonableness. Dr. Hill is the expert who will
18 be or has provided testimony and report explaining
19 why LabMD's practices were not reasonable.
20 BY MR. SHERMAN:
21 Q I guess what I'm trying to find out is
22 whether or not the Bureau is adopting Dr. Hill's

1 report as what would have been reasonable for LabMD
2 to do, and anything less than what she has set out
3 would have been considered unreasonable by the
4 Bureau?
5 MS. VAN DRUFF: Objection; asked and
6 answered.
7 You may answer.
8 THE WITNESS: I don't think we're opining
9 on a hypothetical situation where if LabMD did A,
10 but not B and C, would it have been reasonable.
11 That's not what she's opining on. She looked at
12 their data security practices as a whole and has
13 reached the conclusion that they were not
14 reasonable.
15 BY MR. SHERMAN:
16 Q So she's reached the conclusion that they
17 were not reasonable based on the information that
18 she reviewed?
19 A She sets forth a lot of information that
20 she reviewed, correct.
21 Q So if some other entity looks at
22 Dr. Hill's report as it relates to the LabMD case,

1 is it the Commission's position that the report and
2 the facts in this case will be instructive to a
3 similarly situated entity as to what is expected by
4 the Commission or the Bureau with regard to data
5 security?
6 MS. VAN DRUFF: Objection, Counsel. With
7 respect -- may I actually have the question read
8 back.
9 (Record read by the court reporter as
10 requested.)
11 MS. VAN DRUFF: Counsel, I think it's
12 clear that the Court's ruling in this case allows
13 you to inquire of Mr. Kaufman about the legal
14 standards applied in this case, but it also makes
15 clear that the mental processes of staff, including
16 Bureau staff and Commission staff with respect to
17 other investigations, is not a proper line of
18 inquiry.
19 So possibly I misunderstand your question,
20 but if you can restate it, and then perhaps I can
21 let Mr. Kaufman answer it.
22 BY MR. SHERMAN:

1 Q Well, Mr. Kaufman, you've testified that
2 the source for information for a company like LabMD
3 that has been published are settlements, speeches,
4 blogs, the business educational materials that are
5 on the Web site.
6 My question is, if that information is
7 instructive as to what the Commission would expect
8 of an entity, would you also consider Dr. Hill's
9 report to be instructive in terms of an entity
10 looking at that and trying to discern what the FTC
11 expects in terms of data security?
12 MS. VAN DRUFF: Without revealing the
13 legal reasoning or mental processes of staff or the
14 Commission, you may answer the question.
15 THE WITNESS: I would say that there
16 are -- it would be instructive to other entities to
17 look at her report and get a sense of the kind of
18 issues that the Commission looks at. I will leave
19 it at that. And I should say that the Bureau looks
20 at, because I'm testifying for the Bureau.
21 BY MR. SHERMAN:
22 Q Are there other reports like Dr. Hill's

1 that have been published on the Commission Web site?
2 MS. VAN DRUFF: Objection; vague as
3 to "like Dr. Hill's."
4 MR. SHERMAN: Expert witness reports
5 outlining deficiencies found in an entity's data
6 security.
7 THE WITNESS: I'm not aware of an expert
8 report at the level of detail like Professor Hill's.
9 That said, our complaints do provide a
10 good deal of information regarding the adequate data
11 security practices that were the subject of an FTC
12 lawsuit.
13 BY MR. SHERMAN:
14 Q So it's the Commission's or the Bureau's
15 position that an entity reading the LabMD complaint
16 could find instructive information in terms of data
17 security expectations of the Commission?
18 A I think it is one of the things they could
19 certainly look at, as well as other materials and
20 other source documents that exist outside of the
21 FTC's Web site.
22 Q What kind of other source documents are

1 you referring to?
2 A It could be materials from SANS, from
3 NIST, hardware/software manufacturers. There's a
4 lot of information out there on data security.
5 Q I may have asked you this before, but I
6 need to ask it again. Has the Commission or the
7 Bureau published information informing the general
8 business public that they should look at SANS and
9 NIST and hardware/software product literature, as
10 well as the FTC's business education materials,
11 attend FTC seminars and speeches, and follow the FTC
12 blog and follow the FTC testimony before Congress in
13 order to determine what the FTC or the Bureau
14 considers to be reasonable data security practices?
15 A We certainly haven't said that an entity
16 needs to do all of those things to be aware of it,
17 but certainly, we have issued a lot of different
18 materials that have set forth how we look at data
19 security cases.
20 Q So there's been no -- and you correct me
21 if I'm wrong. There's been no specific announcement
22 or pronouncement or even a warning letter saying

1 hey, business community, if you're not looking at
2 what the FTC is saying about data security, you are
3 likely to not be complying, so you need to look at
4 our business education materials, our testimony
5 before Congress, our settlements that are on our Web
6 site, the speeches that commissioners give, you need
7 to look at our blogs, you need to look at SANS,
8 NIST, check your hardware/software product
9 literature in order to get an idea of what the FTC
10 and the Bureau's data security requirements are.
11 MS. VAN DRUFF: Objection; argumentative.
12 You may answer.
13 THE WITNESS: We have issued in connection
14 with probably all of our data security cases press
15 releases describing the cases, describing the data
16 security inadequacies. We've provided links to our
17 business educational materials, links to blogs.
18 Some of the speeches have been probably subject to
19 press releases but more likely posted on Web sites.
20 As well as the Congressional testimony, we've issued
21 press releases for all of those. And I view those
22 as announcements. So I kind of disagree with the

1 proposition you're starting with there.
2 BY MR. SHERMAN:
3 Q So it's the Commission and the Bureau's
4 position that it has put business entities on notice
5 that they should be looking at all of these types of
6 materials that you've testified here today in order
7 to discern, have some idea of what the Commission's
8 or the Bureau's data security standards are?
9 MS. VAN DRUFF: Misstates prior testimony.
10 You may answer.
11 THE WITNESS: We have provided a lot of
12 outreach that has set forth the availability of this
13 kind of information about reasonable data security
14 on our Web site, and that information has been out
15 there.
16 BY MR. SHERMAN:
17 Q When you say "outreach," what are you
18 referring to?
19 A I'm referring to everything from press
20 releases, media interviews, speeches, Congressional
21 testimony, things of that nature.
22 MR. SHERMAN: Can we take ten minutes?

1 THE WITNESS: Sure.
2 (Recess.)
3 BY MR. SHERMAN:
4 Q Mr. Kaufman, is there a data security
5 standard that the Commission or the Bureau applies
6 to business entities that deal with data that
7 contains sensitive information?
8 A Yes, the Bureau and the Commission have
9 consistently applied the reasonableness standard in
10 the FTC Act.
11 Q So does the term "data security" appear in
12 Section 5 of the Act?
13 A No, it does not.
14 Q So in order for a business entity to
15 determine what data security requirements the FTC
16 would look at, would the Commission advise that
17 entity to look at the FTC Web site, to follow the
18 FTC blog, to research FTC testimony before Congress,
19 to look at the FTC's business education materials
20 that have been published, to consult SANS, to
21 consult NIST, and to look at their hardware/software
22 product literature?

1 MS. VAN DRUFF: Objection; calls for a
2 legal conclusion, vague.
3 You may answer.
4 THE WITNESS: These are among the items
5 that exist where businesses can get a better sense
6 of how the Commission applies its reasonableness
7 standard, but I'm sure there are other sources as
8 well that exist.
9 BY MR. SHERMAN:
10 Q So is it fair to say that there is maybe
11 contained in a speech somewhere this idea has been
12 communicated to business entities that all of the
13 sources I named in the prior question should be
14 consulted when that business entity is trying to
15 determine what data security it should put in place
16 in order to comply with the reasonableness standard
17 of the Act?
18 Can you read that back, please.
19 A Yes. Thank you.
20 (Record read by the court reporter as
21 requested.)
22 MS. VAN DRUFF: Objection; calls for a

1 legal conclusion, vague.
2 You may answer.
3 THE WITNESS: The Bureau has consistently
4 made it clear that those are materials that exist
5 that businesses can look at to get a better sense of
6 how the Commission evaluates what is reasonable data
7 security.
8 BY MR. SHERMAN:
9 Q It's correct, isn't it, that the FTC or
10 the Bureau determines whether a business entity's
11 data security practices were reasonable by
12 investigating what those practices were prior to
13 filing its formal complaint?
14 MS. VAN DRUFF: I caution Mr. Kaufman that
15 he may respond to the question as a general matter,
16 but the reasoning or mental processes of the Bureau
17 regarding its reasonableness determinations in any
18 given case is privileged.
19 THE WITNESS: Can I hear the question
20 again, please.
21 (Record read by the court reporter as
22 requested.)

1 THE WITNESS: Yes, the Bureau will
2 investigate the reasonableness of an entity's data
3 security practices before filing a complaint --
4 before seeking Commission authority to file a
5 complaint, I should say.
6 BY MR. SHERMAN:
7 Q And the Bureau, similar to the business
8 entities, do not have one set of documents that it
9 looks to when determining the reasonableness of a
10 business's security practices? In fact, the Bureau
11 must do what you've suggested the business entities
12 do, which is to consult with all of the various
13 sources that are out there in order to make that
14 determination?
15 MS. VAN DRUFF: Objection; misstates prior
16 testimony. You may answer.
17 THE WITNESS: The sources that are out
18 there that we've been talking about are pretty
19 consistent in how they describe the Commission's
20 approach to assessing reasonableness and data
21 security.
22 There was something else I wanted to say,

1 but it just escaped my mind, if I could hear the
2 question again.
3 (Record read by the court reporter as
4 requested.)
5 THE WITNESS: Yeah, I would just add that,
6 obviously, the issue of data security is an issue
7 that is fact specific, and that changes fairly
8 frequently. So it's not something that there is
9 just a list that exists.
10 BY MR. SHERMAN:
11 Q It's correct that the FTC has not
12 promulgated regulations with regard to data security
13 for personal identifying information?
14 A In connection with Section 5 of the FTC
15 Act, that is correct. We have, nevertheless,
16 consistently applied Section 5 and the unfairness
17 test to assess the reasonableness of the security
18 practices.
19 Q But that's not promulgation of regulation;
20 is that correct?
21 A Yes. Sorry.
22 Q And it's also correct that the Commission

1 nor the Bureau has specifically taken into
2 consideration any different data security standards
3 for HIPAA-covered entities?
4 A Can I hear that back.
5 (Record read by the court reporter as
6 requested.)
7 MS. VAN DRUFF: Objection; vague as
8 to "different."
9 MR. SHERMAN: Let me reword that.
10 THE WITNESS: Okay. Thanks.
11 BY MR. SHERMAN:
12 Q That in terms of applying the fairness
13 standard and looking at the published information
14 out there to determine whether an entity's data
15 security practices comply with Section 5, the
16 Commission nor the Bureau give any special
17 consideration as to whether or not that entity is a
18 HIPAA-covered entity?
19 MS. VAN DRUFF: Objection; vague as
20 to "fairness standard" and "special consideration."
21 You may answer.
22 THE WITNESS: As I said earlier, I'm not

1 aware of any materials that specifically focus on
2 HIPAA entities.
3 But that said, our materials deal with the
4 reasonableness of data security with respect to
5 sensitive personal information, of which the kind of
6 information that HIPAA entities have certainly comes
7 within the ambit of sensitive personal information.
8 BY MR. SHERMAN:
9 Q And so the same analysis would apply to,
10 for example, a Neiman-Marcus, which is high-end
11 retail and doesn't deal with personal health
12 information, as it would to a LabMD, which is a
13 medical lab that solely deals with personal health
14 information?
15 MS. VAN DRUFF: Objection, Counsel. Can I
16 ask you to rephrase the question so it doesn't
17 relate to a specific entity to the extent that
18 they're -- it may raise concerns for Mr. Kaufman in
19 responding?
20 MR. SHERMAN: That's true. I didn't
21 think --
22 THE WITNESS: How about ACME Tool and Die?

1 Let's go to Roadrunner.
2 BY MR. SHERMAN:
3 Q Can we change Neiman-Marcus to ACME Tool
4 and Die, have some fun with this?
5 A If both companies were being looked at
6 from --
7 MS. VAN DRUFF: I'm sorry to interrupt,
8 Mr. Kaufman.
9 Just so the record is clear, can I ask you
10 to restate the question so that there's a clean Q
11 and A?
12 MR. SHERMAN: Yes.
13 BY MR. SHERMAN:
14 Q So is it fair to say that the data
15 security standards that you would apply to a
16 company, for example ACME Tool and Die which
17 specifically deals with retail and the personal
18 identifying information that they receive regarding
19 a purchase at retail, it would be the same analysis
20 that you would do for a company like LabMD, who is a
21 medical laboratory and all of the personal
22 identifying information that it receives is

1 protected health information? The analysis would be
2 the same?
3 MS. VAN DRUFF: Objection; lacks
4 foundation.
5 You may answer.
6 THE WITNESS: The reasonableness analysis
7 that is a part of Section 5 would require a
8 case-by-case analysis of the specific facts of both
9 entities, but they would both be subject to the same
10 reasonableness analysis. But again, it is case
11 specific based on different factors.
12 BY MR. SHERMAN:
13 Q And therefore, the fact that an entity
14 like LabMD has HIPAA regulations to comply with is
15 not a factor that is taken into consideration when
16 the Bureau is analyzing its fairness standard?
17 MS. VAN DRUFF: Objection; misstates prior
18 testimony, lack foundation.
19 You may answer.
20 THE WITNESS: Can I hear that one more
21 time.
22 (Record read by the court reporter as

1 requested.)
2 THE WITNESS: I'm not quite sure how to
3 answer that. Certainly, our analysis ultimately is
4 the unfairness test and reasonableness, but I just
5 don't know how to answer it beyond that.
6 BY MR. SHERMAN:
7 Q Well, you are aware that it is the
8 Bureau's position in this case that HIPAA and HITECH
9 regulations are irrelevant; correct?
10 MS. VAN DRUFF: Objection, Counsel. Do
11 you want to point Mr. Kaufman to a specific
12 document?
13 MR. SHERMAN: No. I'm asking if he is
14 aware that that is the Bureau's position.
15 MS. VAN DRUFF: I'm sorry. I thought you
16 were asserting that it is the Bureau's position.
17 THE WITNESS: I am aware that we are
18 bringing this action under the FTC Act and not under
19 HIPAA or HITECH. So to the extent that the focus is
20 on the FTC Act, that is the focus of the case and
21 not other acts that we're not litigating under.
22 MR. SHERMAN: Okay. I think that's all I

1 have. Kent? That's it.
2 THE WITNESS: Okay.
3 MS. VAN DRUFF: Thank you.
4 (Whereupon, at 11:26 a.m., the deposition
5 was concluded.)
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

EXHIBIT 34

Expert Report of Adam Fisk
In the Matter of LabMD, Inc.
FTC Complaint #1023099, Docket #9357

Table of Contents

Executive Summary 3

Summary of Experience and Qualifications 4

Networking Fundamentals 6
TCP Connections 6
Firewalls 7

LimeWire Overview 9
Sharing Files or Folders 10
Search 13
Browse Host 16

The LabMD Network and Policies in Detail 16
Information Technology (IT) Outsourcing 17
The ZyWALL 5 IPSec Firewall 17
The Cisco 1841 Integrated Services Router 20
LabMD's User Account Policies 22

The 1,718 File 23

Rebuttal to the Expert Report of Raquel Hill, PH.D. 26

Conclusion 32

Appendix A: CV 35

Appendix B: Materials Considered or Relied Upon 37
Deposition Transcripts and Exhibits 37
Correspondence 37
Bates Range 37

Executive Summary

I am the former Lead Engineer at LimeWire LLC, the creators of the LimeWire file sharing application, and an expert in peer-to-peer software, computer networking, and data security. I am currently the President and CEO of the Brave New Software Project, Inc., the creators of Lantern, a peer-to-peer tool for bypassing government censors in countries such as Iran and China that censor citizens' access to the Internet. Lantern is funded through over $4 million in grants from the U.S. State Department and U.S. AID. The Brave New Software Project, Inc. has also partnered with Google, Inc. in the creation of the uProxy tool for bypassing Internet censors.[1]

The Respondent has retained me as an expert witness in the defense of LabMD, Inc. ("LabMD") against the Federal Trade Commission. The Respondent has asked me to provide an opinion as to whether LabMD provided adequate security to secure Protected Health Information[2] contained within its computer network from January 2005 to July 2010 ("Relevant Time Period").

This report contains my findings and the logic underlying those findings. In addition, it contains:

- A summary of my qualifications
- An overview of LimeWire functionality
- An analysis of the LabMD network
- An analysis of the 1,718 file on the LabMD network
- A rebuttal to the expert witness report of Raquel Hill, PhD

[1] uProxy, https://www.uproxy.org.
[2] LabMD, Inc. as a "covered entity" under HIPAA utilizes and possesses Protected Health Information "PHI". Complaint Counsel refers to this as personal information.

Based on my review of the documentation in this case, it is my opinion that LabMD implemented appropriate security measures to secure the Protected Health Information in its possession during the Relevant Time Period.

Summary of Experience and Qualifications

I have 13 years of professional experience building peer-to-peer applications with a focus on computer networking and security. I received my BA degree in Computer Science and US History from Brown University. After graduating from Brown, I moved to New York, NY to join LimeWire LLC in June of 2000 several weeks after its creation. I became the Lead Engineer in 2002. During my time at LimeWire, I authored or co-authored all of the specifications for how search worked on the modern day Gnutella network.[3] Those specifications are still deployed on the Gnutella network today. I also helped to implement virtually all aspects of the LimeWire software, including but not limited to searching, downloading, the user interface, and creating the installers.

I left LimeWire in February 2004 to co-found Last Bamboo LLC, a software startup dedicated to building a next-generation peer-to-peer platform that would address many of the shortcomings of peer-to-peer ("P2P") software at the time, particularly LimeWire and BitTorrent. Last Bamboo built the LittleShoot file sharing application that integrated BitTorrent seamlessly with the web browser and received coverage in the New York Times, Mashable, and LifeHacker.[4] The LittleShoot platform adopted emerging voice-over-IP ("VoIP") standards for penetrating Network Address Translators ("NATs")

---

[3] *See* Adam Fisk, *Gnutella Dynamic Query Protocol v0.1*, May 2003, https://lantern.s3.amazonaws.com/dynamic_query.html; and Adam Fisk, *Gnutella Ultrapeer Query Routing v0.1*, May 2003, https://s3.amazonaws.com/lantern/ultrapeer_qrp.html

[4] LittleShoot, http://www.littleshoot.org

and firewalls that were far more effective than the techniques used in other P2P tools. In doing so, I provided feedback on and helped to revise several of the Internet standards governing VoIP on the Internet, including the Session Traversal Utilities for NAT ("STUN") and Interactive Connectivity Establishment ("ICE") protocols at the Internet Engineering Task Force ("IETF").

In the summer of 2010, I began work on using the LittleShoot platform to bypass government censors around the world in their efforts to censor the Internet, including countries such as Iran, China, Bahrain, Vietnam, Thailand, Turkey, etc. I founded the Brave New Software Project, Inc. ("BNS") as an entity under which to build this new tool. BNS's mission is to use software to tackle tough global problems. The work on bypassing censors came to be called Lantern, and it is the first such tool. Lantern uses P2P, trust networks, and a number of Internet networking nuances to provide Internet access to web sites that would otherwise be blocked, such as youtube.com, facebook.com, and twitter.com in both Iran and China. As of this writing, it is the only known tool that continues to work in the face of countermeasures from both the Chinese and Iranian governments, both of whom have far more resources than BNS at their disposal. Lantern is open source and is designed to stay unblocked even if censors know exactly how it works. It uses fundamental design principles that take advantage of the inherent Internet architecture. I am therefore intimately familiar with the hardware and software tools and mechanisms used to secure networks and how to circumvent them.

Lantern is funded through a $2.2 million dollar three year grant from the US State Department and a pending $2.4 million dollar grant from US AID. We have also worked closely with Google, Inc. on a new tool called uProxy that uses similar techniques for

getting around censors.[5] I have spoken about Lantern at conferences around the world, including TEDx[6] and the Nantucket Project.[7]

Networking Fundamentals

When assessing the adequacy of LabMD's security, it is important to have a basic understanding of some fundamental concepts in computer networking and security. This analysis will focus on the networking and security concepts relevant to this case and will particularly leave out a more exhaustive description of all computer networking concepts such as switches, routers, MAC addresses, etc, that have no impact on the analysis of LabMD's network security and its adequacy. There are many networking details that are common to all computer networks, like the computer network that LabMD operated.

TCP Connections

The Transmission Control Protocol (TCP) is the core protocol that powers most computer network traffic. When you open a web browser to www.google.com, for example, your web browser opens a series of TCP network connections from your computer to Google. Those connections fetch the data that displays www.google.com in your web browser. TCP connections are opened in a directional fashion from one computer to another.[8] This connection is technically from one Internet Protocol (IP)

---

[5] uProxy, https://www.uproxy.org.
[6] *See* Adam Fisk, *Internet Freedom by Design*, September 2013, https://www.youtube.com/watch?v=PpwSJDdo6Vs
[7] The Nantucket Project, Adam Fisk, https://www.nantucketproject.com/adam-fisk.
[8] Technically network traffic flows between the Network Interfaces Cards between two computers.

address and port pair to another IP and port pair, such as the following showing a connection from IP address 4.4.4.4 and port 7777 to IP address 5.5.5.5 and port 8888.

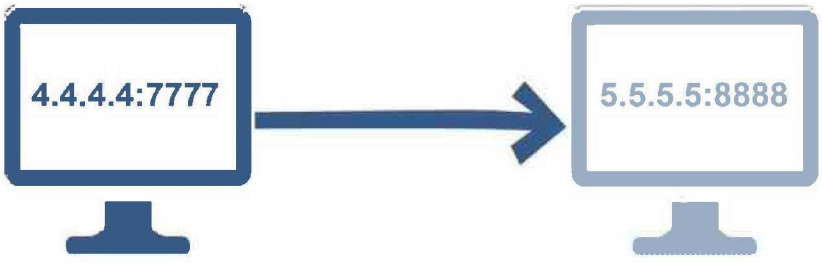


Figure 1

Conceptually this is very similar to mailing a physical letter from one address to another. The computer at 4.4.4.4:7777 is the sender with a return address, and the computer at 5.5.5.5:8888 is the recipient of the letter. For the purposes of this analysis, it is important to understand that the *establishment* of the network connection is *directional* with a distinct sender and a distinct receiver. Once the connection is established, traffic flows in both directions, but creating the initial connection starts at one computer and ends at the other.

Firewalls

The above description of TCP connections and particularly the notion that they are established from one side to the other is fundamental to the concept of firewalls. The figure below depicts two networks without any firewalls between them. It shows how TCP connections can be made freely in either direction between the two computers.

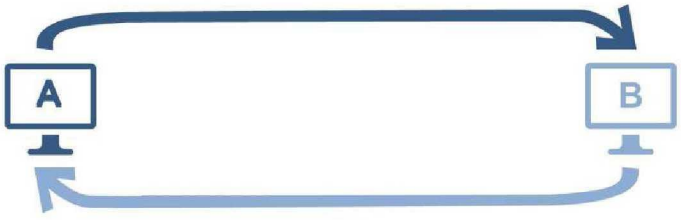


Figure 2: With no firewalls between computers A and B, network connections (TCP connections) can be made freely in either direction.

In contrast to the no-firewall example, if computer A is behind a firewall it can make *outgoing* connections to computer B, but the firewall will block *incoming* connections from computer B. This is depicted in the following figure.

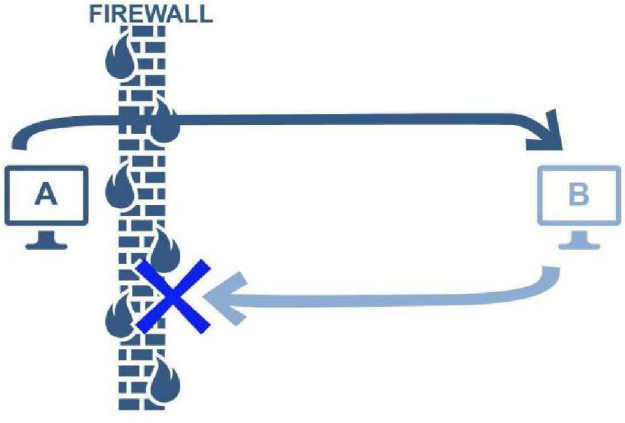


Figure 3: This depicts how firewalls will allow outgoing connections but will disallow incoming connections, just as a Congressional office building might screen incoming mail but send all outgoing mail. In the figure, the Congressional office building would be analogous to computer A.

Firewall configurators can choose to configure firewalls to also block outgoing connections, but this is atypical because when a network is connected to the Internet at all it is typically because, well, you want to make network connections to the Internet. A

good example of this is e-mail. If a company uses any web-based e-mail client, such as Gmail, employees' web browsers must make outgoing network connections to mail.google.com (corresponding to Computer B in Figure 3). If the firewall blocked those connections, employees' e-mail would simply not work.

This default functionality of all firewalls is again analogous to physical mail. If you receive mail in a location where you might expect threats to arrive by mail, such as a Congressional office building, it is common practice to screen that incoming mail. This is very similar to how a firewall screens incoming network traffic, although a firewall is much more extreme and simply blocks all incoming traffic by default. It is only in the most extreme circumstances, such as perhaps in a prison, that outgoing mail is screened in the same fashion. Firewalls similarly allow all outgoing connections by default but can be further locked down in extreme circumstances. This understanding of firewalls is fundamental to LabMD's security more generally and also to the specific case of the file sharing software LimeWire, as discussed in the following section.

LimeWire Overview

LimeWire is a peer-to-peer file sharing application used to transport files across the Internet. LimeWire is one of a number of applications that use a protocol called Gnutella. Gnutella connects computers together in a direct peer-to-peer fashion to facilitate file sharing through searching and downloading.

- **Sharing a file or folder**: The ability to share a file or folder on the network.
- **Search**: The ability to search for shared files on hundreds of thousands of other computers on the network in a distributed fashion

- **Browse host**: The ability to view all of the files a specific peer computer is sharing on the network

We will review each of these pieces of functionality in detail.

Sharing Files or Folders

In order to share a file or folder on LimeWire, the user must actively choose the file or folder to share. If a user chooses an entire folder, LimeWire could facilitate the sharing of the files within that folder and by default any subfolders as well. As shown in the following figure, the user must click on the "Add Files" button from within the application.

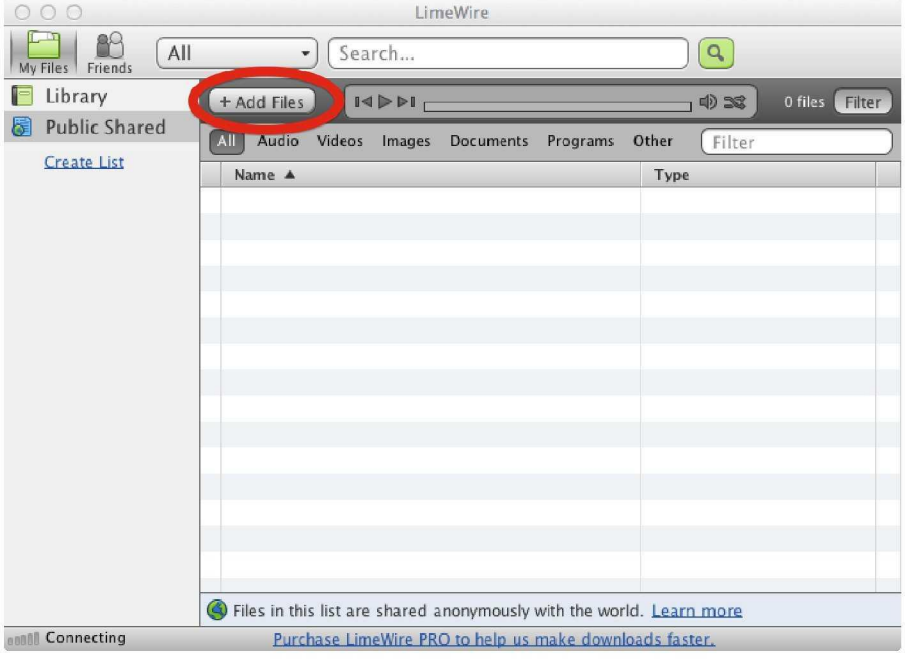


Figure 4: Sharing a file or folder using LimeWire

When the user clicks the "Add Files" button, he or she is able to select the file or folder to share on his or her computer. In the following figure, the user selects the "folder-to-share" folder to permit sharing of all the files within that folder.

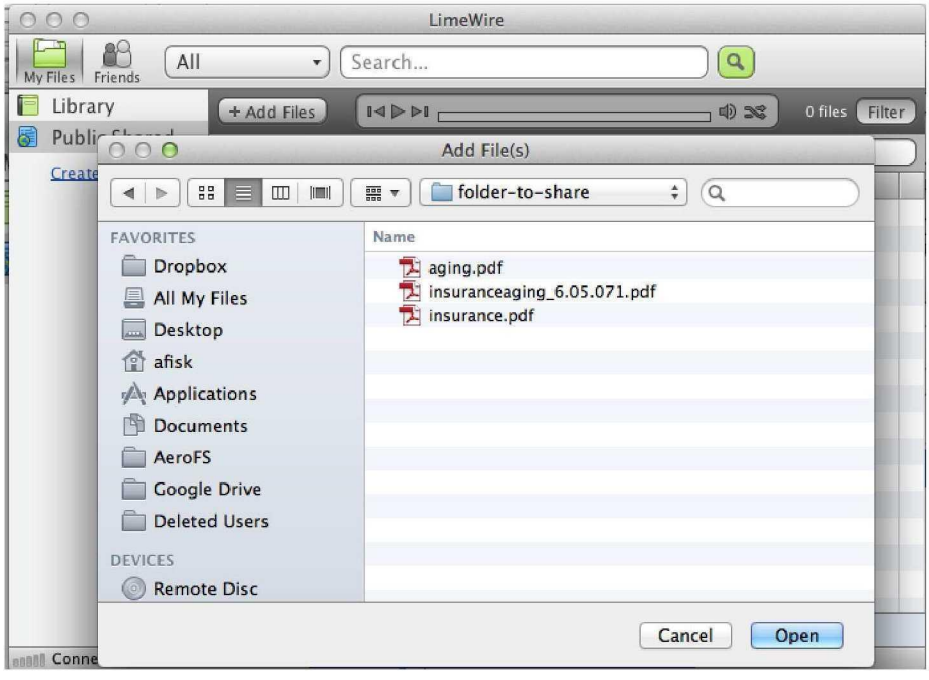


Figure 5: User actively selecting the "folder-to-share" folder to share on the network. As seen in the image, the folder contains three files.[9]

As seen in the figure, the folder contains the following three files:

1. aging.pdf
2. insuranceaging_6.05.071.pdf
3. insurance.pdf

This example intentionally uses the file name "insuranceaging_6.05.071.pdf" for one of the shared files to illustrate the process required to share that file through LimeWire and precisely what happens when a search for that file takes place.

When the user makes these three files searchable on LimeWire, LimeWire breaks apart the file names into keywords that will allow other users to search for them. In this case, LimeWire simplifies the "aging.pdf" file to the keyword "aging" and will match searches for the term "aging." Similarly, the "insurance.pdf" file translates to the

[9] This is not an actual screenshot of the LabMD computer at issue.

keyword "insurance" being shared. Similarly the "insuranceaging_6.05.071.pdf" file will be simplified into the keyword "insuranceaging" and "6.05.071" because LimeWire only recognizes the "_" as a word delimiter and does not recognize that "insuranceaging" is, in fact, the words "insurance" and "aging" merged together. This understanding is vital to understanding the description of search on LimeWire and the Gnutella network in the following section.

This example illustrates several important points. First, the user must actively choose a folder or specific file on LimeWire. This is a deliberate action. In the case of LabMD, the evidence indicates that the billing manager, Rosalind Woodson, chose to make the My Documents folder searchable and within that folder the aforementioned insuranceaging_6.05.071.pdf file.[10] LimeWire does not share the My Documents folder by default, and Ms. Woodson would have had to deliberately configure it to do so.

Beyond the degree to which sharing the folder containing insuranceaging_6.05.071.pdf was a deliberate action, this example also illustrates the unique and difficult to find nature of that particular file as a result of its unusual name. To fully understand this point it is necessary to understand the nature of searching through LimeWire, as discussed in the following section.

[10] While the evidence shows that Ms. Woodson made the 1718 file searchable on LimeWire, no evidence exists that the file was actually shared with anyone on LimeWire.

Search

As described in the section on sharing, the act of sharing a file breaks the file name apart into keywords that are then available for search. The above example results in the following keywords being shared on the network:

1. insurance
2. aging
3. insuranceaging
4. 6.05.071

A search for "insurance" would only return a result for the "insurance.pdf" file. Similarly, a search for "aging" would only return a result for the "aging.pdf" file. In particular, neither of those searches would return a search result for "insuranceaging_6.05.071.pdf". In order for the searcher to receive a search result for the "insuranceaging_6.05.071.pdf" he or she would have to enter the search terms "insuranceaging" or "6.05.071". Both of those searches are highly unusual, and it is extremely unlikely that any LimeWire user would ever enter them. In particular, none of the search terms enumerated in Eric Johnson's report would ever return search results for the insuranceaging file.[11] To think that any of those search terms would provide a search result for the aforementioned file simply reflects a lack of understanding of how search technically works on LimeWire and the Gnutella network.

To adequately conceptualize this functionality, it is useful to be able to picture the Gnutella network topology upon which LimeWire operates. Each computer on the Gnutella network forms connections to other computers, with computers behind firewalls initiating outgoing connections to computers not behind firewalls as previously

[11] M. Eric Johnson, *Data Hemorrhages in the Healthcare Sector*, Financial Cryptography and Data Security, February 22-25, 2009, at Figure 7.

discussed. Once those connections are established, computers are able to send messages to a larger number of computers on the network, even though they are not directly connected, because a computer's direct network connections will forward them to their own connections.

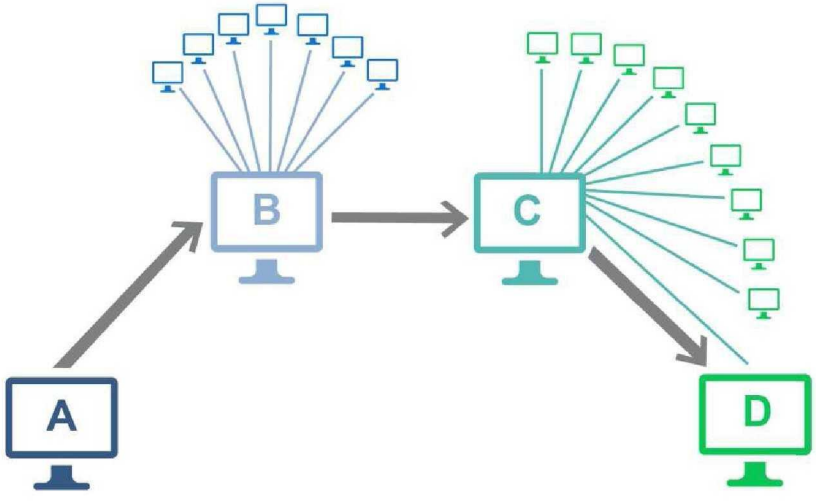


Figure 6: LimeWire/Gnutella network topology. Computer A is able to send messages to Computer D because Computer A has network connections to Computers B and C, and Computers B and C forward the messages from A. Those messages could be searches or other types of messages.

In the figure, Computer A is able to send a message to Computer D because the Gnutella protocol dictates that Computer B forwards the search to Computer C, which in turn forwards the search to Computer D.[12]

The figure depicting the Gnutella network topology is useful for conceptualizing the network as a whole. Picture approximately the same image, but multiplied 500,000 times. The result would more closely reflect the Gnutella network in the real world. On

[12] In reality the search is only forwarded if the next computer is actually sharing a keyword matching the search term. This uses a relatively complicated process of distributed indexing of keywords using what are called Bloom Filters, however, that is an unnecessary distraction for the purposes of this analysis.

such a network, several other factors have to coincide for a search to successfully find a file:

(1) the computer sharing the file has to be online;

(2) the computer sharing the file has to be running LimeWire;

(3) the searcher has to utilize a search term that will find the file; and

(4) both the searcher and the user sharing the file have to relatively close to each other on the network.

This latter point is the result of the "Adaptive Search" protocol I authored for the Gnutella network and implemented in LimeWire. [13] This protocol takes several factors into account. First, it recognizes that the network is so large that having any searches reach every single computer on the network would quickly consume too many network resources, leaving individual computers potentially overloaded and leaving little bandwidth for other purposes. As a result, Adaptive Search limits the total reach of any single search to a maximum of approximately 300,000 computers. At any one time on the LimeWire network there would be approximately 2 to 5 million users online. As **such,** **searches would reach a *maximum* of anywhere from approximately one sixth to approximately one fifteenth of the total network**. In addition, the Adaptive Search protocol takes into account the number of search results received. A search for "Beatles", for example, would result in a large number of search results. In that case, the Adaptive Search protocol would quickly recognize the large number of search results arriving and would stop the search well before reaching 300,000 computers. In the case of searches for

[13] Adam Fisk, *Gnutella Dynamic Query Protocol v0.1*, May 2003, https://lantern.s3.amazonaws.com/dynamic_query.html.

particularly popular content such as "Beatles", the search may only reach a couple of hundred computers or less.

Given the nature of keyword matching on Gnutella and the nature of Adaptive Search, it is my opinion that it is extremely unlikely that any *typical* user of the Gnutella network, including highly sophisticated users, would ever have found the "insuranceaging_6.05.071.pdf" file in question using search alone.[14]

Browse Host

LimeWire contains another feature referred to as "browse host." Browse host allows one LimeWire user to view all the files another LimeWire user has made available to share. In order to download the files of a browse host either the Downloader or the Uploader must not be behind a firewall. Once the browse host message succeeds, the Downloader is able to see all of the files the Uploader is sharing. The Downloader can then choose to download any of those files.

The LabMD Network and Policies in Detail

The network deployed at LabMD during the Relevant Time Period contained the basic components one would expect to find at most small businesses operating at the time. This included routers, switches, firewalls, servers, and employee computers. Switches, computers, and the raw cables connecting them are the basic components of any network. Switches and cables turn a collection of independent computers into a computer network. Routers in turn simply connect one network to another network. For

[14] *See* Robert Boback Deposition, November 21, 2013 Deposition Transcript, pp. 117

example, a router can connect a local area network (LAN), such as the network in an office, to the Internet. All of these components are common to any network connected to the Internet, and their existence at LabMD was simply indicative of the fact that LabMD ran a computer network connected to the Internet. The issue at hand involves the adequacy of the security components, policies, and practices built around those fundamental networking components. That is what we will address in this section.

Information Technology ("IT") Outsourcing

The material I have read in compiling this report makes it clear that LabMD outsourced the majority of its IT infrastructure. The two primary vendors LabMD employed during the Relevant Time Period were Automated PC Technologies (APT) and Cypress Communications. Each of these vendors provided hardware for the most critical part of LabMD's network, namely the interface between the local network (LAN) and the Internet. The components controlling that interface are so critical because that interface separates the trusted network from the untrusted network.

The ZyWALL 5 IPSec Firewall

To protect the interface between the trusted internal network and the untrusted Internet, APT installed several ZyWALL 5 IPSec firewalls.[15] These firewalls protected servers and employee computers from *incoming* network traffic.[16],[17] The ZyWALL 5 IPSec manual even for the early 2004 models describes this functionality and default

[15] Truett Dep. at 58.
[16] See Hyer Dep. at 91.
[17] Truett Dep. at 41.

configuration clearly. Even those earliest available versions disallowed all incoming TCP traffic by default.[18] The following diagram from the ZyWALL 5 datasheet depicts its general place on a network.

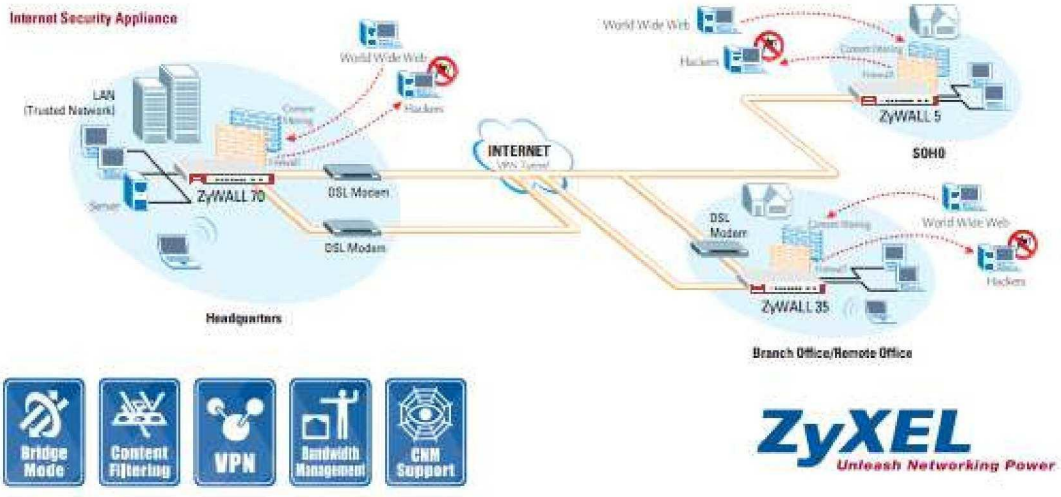


Figure 7: The ZyWALL 5 VPN and Firewall, shown in the top right, includes firewall capabilities as well as the ability to mitigate against distributed denial of service ("DDOS") attacks and to filter content using state of the art BlueCoat filtering technology.[19]

The ZyWALL 5 user guide provides further confirmation that it blocks incoming network requests while allowing outgoing requests by default, just like almost any firewall.

---

[18] ZyXel Communications Corporation, *Zywall 5 Internet Security Appliance: Users Guide* §9.5.3 TCP Security (Version 3.62 2004), available at: ftp://ftp2.zyxel.com/ZyWALL_5/user_guide/ZyWALL%205_3-62.pdf

[19] ZyXel Communications Corporation, *Zywall 5 Internet Security Appliance: Users Guide* (Version 3.62 2004), available at: ftp://ftp.zyxel.com/ZyWALL_5/datasheet/ZyWALL%205_1.pdf.

10.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

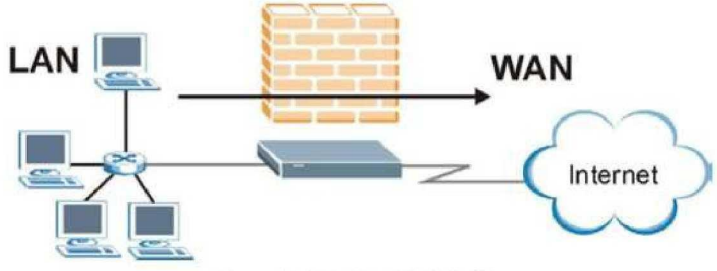


Figure 10-1 LAN to WAN Traffic

10.4.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

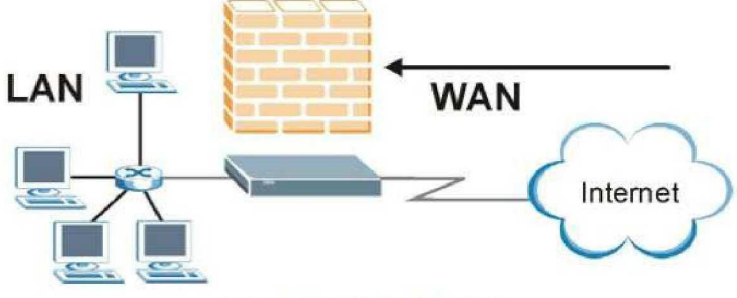


Figure 10-2 WAN to LAN Traffic

Figure 8: Description of default firewall rules in the ZyWALL 5 user guide. The user can change these defaults but would have to create a custom rule to explicitly allow LimeWire traffic in from the WAN, which you would simply never do. [20]

[20] ZyXel Communications Corporation, *Zywall 5 Internet Security Appliance: Users Guide* §10-3 (Version 3.62 2004), available at: ftp://ftp2.zyxel.com/ZyWALL_5/user_guide/ZyWALL%205_3-62.pdf.

It is my opinion that the ZyWALL 5 was more than adequate for serving the needs of a small business like LabMD, in that **it blocked incoming network requests while allowing outgoing requests by default**. That is what it is designed to do, and anything more would simply be unnecessary for the number of employees the firewall had to service. Beyond providing a firewall, it also provided other security enhancements such as distributed denial of service (DDOS) protection. It would also log apparent attacks and alert network administrators when attacks took place.[21] Just *like any other firewall during the Relevant Time Period*, the ZyWALL 5 would not by default protect against a sophisticated crawl of a network with LimeWire running because that crawl would rely on a connection from LimeWire coming from the LAN to the WAN (Internet), precisely the type of connection the firewall is correctly designed to allow.[22]

The Cisco 1841 Integrated Services Router

The other primary piece of hardware deployed at the interface between the trusted and untrusted network during the Relevant Time Period was the Cisco 1841 Integrated Services Router. Cypress Communications installed, configured, and maintained these routers.[23] It then leased them to LabMD.[24] Cisco's data sheet on 1841 reads as follows:

---

[21] ZyXel Communications Corporation, *Zywall 5 Internet Security Appliance: Users Guide* Version 3.62 2004), available at: ftp://ftp.zyxel.com/ZyWALL_5/datasheet/ZyWALL%205_1.pdf.

[22] To make this clear, it would allow the LimeWire outgoing connection in the same way that it would allow an outgoing connection from a user's web browser to www.google.com. This was not some nefarious behavior on the part of LimeWire but rather the fact that networks generally trust any installed applications to make outgoing connections from the local network to the Internet while restricting incoming access.

[23] Sandrev Dep. at 24.

[24] Sandrev Dep. at Exhibit RX1, Cyprus Communications, Inc., Master Terms and Conditions.

"Cisco Systems® is redefining best-in-class enterprise and small- to-medium-sized business routing with a new line of integrated services routers that are optimized for the secure, wire-speed delivery of concurrent data, voice, and video services." The documentation for the Cisco 1841 is readily available from Cisco's web site, even for the older firmware version 12.4 deployed at LabMD during the Relevant Time Period.[25]

This evidence makes it clear that the 1841 had not only sophisticated firewall capabilities but also *sophisticated intrusion detection capabilities*.[26] In contrast to Curt Kaloustian's testimony that describes the Cisco 1841 as "very rudimentary,"[27] the Cisco 1841 is, in fact, a very sophisticated piece of hardware with a wide variety of functionality designed precisely for the type of small business network in place at LabMD. It runs Cisco's state of the art IOS operating system, including the ability to run the IOS firewall and the IOS intrusion prevention system.[28]

Cypress representative Peter Sandrev maintains that they "instituted what was called an implementation coordinator who would be responsible for a customer's implementation."[29] Given that these routers were the gateways to LabMD's internal network, the implementation coordinator would very likely deploy at least the 1841's firewall capabilities and possibly its intrusion prevention system ("IPS") as well.

---

[25] Sandrev Dep. at 52.
[26] Cisco, Cisco 1841 Router (Modular), http://www.cisco.eom/c/en/us/products/collateral/routers/1800-series-integrated-services-routers-isr/product_data_sheet0900aecd8016a59b.html.
[27] Kaloustian Dep. at 107.
[28] Cisco, Cisco 1841 Router (Modular), http://www.cisco.eom/c/en/us/products/collateral/routers/1800-series-integrated-services-routers-isr/product_data_sheet0900aecd8016a59b.html.
[29] Sandrev Dep. at 47.

It is my opinion that for a company such as Cypress managing such a critical component of a customer's infrastructure to not configure them with at least a firewall in place would be highly unusual. If Cypress was aware of the nature of LabMD's work, it is also quite likely they would have deployed an IPS as well.

Given the capabilities of the Cisco 1841, it is clear that LabMD had all the adequate equipment in place to protect its network from the Internet. Even if the 1841 were erroneously configured to not enable its firewall functionality, the ZyWALL 5 firewalls sitting behind the Cisco 1841s would still have adequately protected the network from incoming network traffic, as already discussed in detail. The LabMD network was thus protected from the Internet through two layers of equipment either one of which I would consider adequate to maintain the security of the LabMD network.

LabMD's User Account Policies

The LabMD policy for assigning accounts to each user on his or her desktop computer is outlined in LabMD's Employee User Account Policy section of the LabMD Computer Hardware, Software and Data Usage and Security Policy Manual. This policy clearly states that ordinary employees are given accounts on their machines that restrict the ability to download files from the Internet and to install software on the computer. This policy was in place as of 2001.[30]

Robert Hyer confirmed this policy in his deposition and also discussed how a small number of management level employees were given user accounts allowing them to

[30] Philippa Ellis Letter, produced at FTC-LABMD 002523-002524.

download files on the Internet and to install additional software on their computer.[31] This was the case for Rosalind Woodson, who because she was a management-level employee likely needed access to unique applications to perform her job duties as the billing manager.[32] Clearly the LimeWire application was not required for her to perform her job, and therefore was a clear violation of LabMD's data security policies.[33]

The 1,718 File

A further analysis of the insuranceaging_6.05.071.pdf, referred to as the 1,718 file, is illustrative of LabMD's security practices more generally. As discussed in detail in the section on LimeWire's search functionality, it is my expert opinion that it is extremely unlikely that any casual user of LimeWire would ever search for either the terms "insuranceaging" condensed together in that manner, or the term "6.05.071". Again, to even originally expose this file in any manner on the network, Rosalind Woodson had to take all of the following steps:

1. Installed LimeWire on her computer even though it clearly violated company policy
2. Actively chosen to share her My Documents folder, which LimeWire did not share by default
3. Actively saved the insuranceaging_6.05.071.pdf file in that folder

Even with all of these steps taken, however, it would still have been almost impossible for anyone on the network to realistically find the file using LimeWire's search functionality.

---

[31] Hyer Dep. at 29-30.
[32] Simmons Dep. at 124-125.
[33] See LabMD Computer Hardware, Software and Data Usage and Security Policy Manual, Employee User Account Policy.

In order for Tiversa to access that file, they would have had to use the browse host function described above. Mr. Boback's testimony also confirms that assessment.[34] No ordinary user of the network would ever have the knowledge of how Gnutella works or the technical capability to take advantage of that knowledge to perform the types of crawls Tiversa performed. Without that capability or knowledge, it is extremely unlikely any ordinary user would ever have found the 1,718 file. **The vital point is that only extremely sophisticated and custom-designed software would ever be configured in this fashion**

Tiversa CEO Robert Boback stated clearly in his deposition that Tiversa did not, in fact, download the 1,718 file directly from LabMD. Instead, the Tiversa crawls originally located the file on a computer at IP address 68.107.85.250 in San Diego.[35] My analysis concludes that only one or more extremely sophisticated network crawlers could have found this file – network crawlers in comparable sophistication to Tiversa itself. In order to find the 1,718 file someone would have to understand the nuances of the browse host message and would have had to have written custom software to take advantage of that knowledge. It is extremely unlikely they would have been a casual user of the network.

If casual LimeWire users did not, in fact, download the file from LabMD, then how did it end up at the IP address 68.107.85.250? One possibility is that there were other equally sophisticated network crawlers operating at those addresses. At that time there were several candidates who might have actually run those types of crawls:

---

[34] Boback Dep. at 117.
[35] Boback Dep. at 29-35.

(1) The FBI was quite rigorously investigating the sharing of child pornography on peer-to-peer networks;

(2) Another was Big Champagne, a company that scoured peer-to-peer networks to determine the popularity of various forms of media; and

(3) Finally, there was the Recording Industry Association of America ("RIAA") and the Motion Pictures Association of America ("MPAA"), or more specifically companies working on their behalf such as Media Defender.

These were copyright holders attempting to locate and prosecute people infringing on their copyrights. **In short, all of these were sophisticated organizations capable of deploying the financial and ultimately technical resources required to locate the 1,718 file and not simply casual LimeWire users.**

The other possibility is perhaps simpler. Instead of the file actually leaving LabMD through LimeWire, an employee could have simply placed that file on a portable storage device, such as a thumb drive, and walked out the door with it. Or that employee could have emailed the file as an attachment to a friend. **Both methods are much less technically sophisticated than downloading the file through a custom network crawl. Thus, if LabMD's only failure is that it did not have adequate measures in place to prevent an employee from downloading a file to a thumb drive and that it did not prevent all employees from having email capabilities, then that is a very high standard indeed and one which I do not believe many small companies could have met in the 2007 - 2008 time frame.**

Rebuttal to the Expert Report of Raquel Hill, PH.D.

In reaching my findings I have reviewed the expert report of Raquel Hill, PH.D. Ms. Hill concludes the following:

> LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures.[36]

Ms. Hill reaches her conclusion, however, based on a number of fundamentally flawed assumptions. First, she has only a rudimentary understanding of how LimeWire works at the network level. In particular, she clearly does not understand the browse host mechanism. As such, her analysis of LabMD's firewall configuration is simply inaccurate. Her lack of understanding in this area is, in fact, indicative of the sophistication both of LimeWire and of the technique used to obtain the 1,718 file and is not due to any failure of integrity on her part.

In her description of "Firewalls and Intrusion Detection Systems," Ms. Hill provides the following accurate description of firewalls:

> Firewalls can also be configured to prevent and/or limit incoming connection requests. An incoming connection request is a request that originates from outside of the network but seeks to establish communication with a computer that is within the network. Only computers that are running authorized server applications should receive connection requests. A firewall, for example, could be configured to prevent all incoming connection requests for computers that are not running an authorized server application.[37]

As I have described, in fact, most firewalls simply block incoming connection requests by default. Most importantly, the ZyWALL 5 IPSec firewall deployed at LabMD during the Relevant Time Period does precisely that. Ms. Hill's description leads to a

[36] Hill, Expert Report, at 18.
[37] Hill, Expert Report, at 7.

conclusion that is simply incorrect; namely that LimeWire was running as an application accepting *incoming* connection requests through the firewall.[38] For this to be the case, the firewall would have to be *radically* misconfigured, with administrators explicitly opening ports to allow files on the network to be downloaded through LimeWire in particular. In fact, however, LimeWire was making authorized *outgoing* connection requests to the Gnutella network. As Ms. Hill states in the above quote, "Only computers that are running authorized server applications should receive connection requests." This is true, and the fact is that the computer running LimeWire did not ever receive any connection requests through the firewall because it was *sending* the connection requests.

This fundamental misunderstanding then goes on to infect the rest of Ms. Hill's analysis. This is clear on page 43 in sections e and f. In section e, Ms. Hill writes:

> A firewall should be employed at the network gateway to block all unwanted traffic from entering the network. The gateway firewall could be configured to block traffic destined to all unauthorized applications, such as file-sharing applications, which in turn would prevent traffic for those applications from entering the network. This type of configuring would create a list of acceptable applications and was routinely done by IT practitioners throughout the Relevant Time Period.[39]

In fact, a firewall was "employed at the network gateway to block all unwanted traffic from entering the network." As described above, the traffic did not enter the network, but rather it left – LimeWire made *outgoing* connections because it knew the firewall would not accept traffic *entering the network*. Further, that firewall was, as Ms. Hill suggests it should be, "configured to block traffic destined to all unauthorized applications, such as file-sharing applications" for the same reason. The firewall was not only employed in this way and configured in this way, but it actually succeeded in

[38] Hill, Expert Report, at 43.
[39] Hill, Expert Report, at 43.

blocking precisely the traffic she describes. The problem is again a misunderstanding of how LimeWire works when it runs from behind a firewall. In that case, it makes *outgoing* connections rather than *incoming*. The ZyWALL 5 IPSec firewall at LabMD blocked *incoming* connections but allowed *outgoing* connections just as it should, again just as any company would send outgoing physical mail without screening it. The list of acceptable applications she mentions is only relevant in a conception of the network that assumes the network connections were *incoming* connections. In fact, the ProviDyn external vulnerability scan conducted on May 21, 2010 showed that the LimeWire port 6346 was not, in fact, open to outside intrusion.[40]

This same fundamental problem is repeated again in section f of page 43, where she states the following:

> In addition, all employee workstations should be configured to use a software firewall. On August 25, 2004, Microsoft released its Windows Firewall as part of Windows XP Service Pack 2. This software firewall could be configured to block all incoming connection requests to a workstation. This would prevent, for example, users of file-sharing applications, like LimeWire, from establishing a successful connection with a workstation and downloading shared files. The Windows Firewall accompanied the operating system at no cost to the customer.[41]

Again, the connections in this case simply were not "incoming connection requests to a workstation." Rather, they were outgoing requests as depicted in Figure 3. If every computer at LabMD were installed and configured in exactly the way Ms. Hill describes, it would have had absolutely zero effect on the ability of LimeWire to share files. In fact, it would have been redundant because there was already a firewall at the

---

[40] ProviDyn External Vulnerability Scan, produced at FTC-LABMD-002753- FTC-LABMD-002754. If the firewall had been configured to allow LimeWire in through it, the port number 6346 would be included in the list of port numbers.
[41] Hill, Expert Report, at 43.

network gateway accomplishing the same function of blocking incoming connections. LabMD was, in fact, implementing the best practice Ms. Hill describes of deploying a firewall to block incoming traffic.

This fundamental issue appears again in Ms. Hill's description of firewalls mapping to specific applications, making it misleading. She states:

> Thus, to illustrate the concept of defense in depth, a first line of defense to prevent use of unauthorized applications is to configure a firewall to close all ports at the gateway router except those that are used by authorized applications.[42]

This statement implies that the firewall had opened incoming ports for the unauthorized application in question, LimeWire. In fact, all evidence indicates that those ports were, in fact, closed[43].

Part of the problem with Ms. Hill's analysis is that it relies heavily on the testimony of Curt Kaloustian. To even a moderately experienced network engineer it would be clear that Mr. Kaloustian had a limited understanding of computer networks, and as such his testimony should be read with a critical eye. For example, he states on page 112 that "ports can be anywhere from zero to 9,999."[44] As anyone with a basic knowledge of computer networking knows, ports in fact range from $0\text{-}2^{16}$ or 0-65,536. Ms. Hill correctly states this port range in her report, and as such she clearly realizes Kaloustian's testimony is not particularly reliable or informed, however she nevertheless cites Kaloustian's testimony to back up her claim on page 45 that "these firewalls were not configured to prevent unauthorized traffic from entering the network." Kaloustian's

---

[42] Hill, Expert Report, at 10.
[43] ProviDyn External Vulnerability Scan, produced at FTC-LABMD-002753- FTC-LABMD-002754.
[44] Kaloustian Dep., at 112.

testimony in fact directly contradicts that statement. On page 101, he states, "these appliances would save to basically manage and route authorized traffic back and forth through them."[45] He also clearly states that he did not perform the configuration when he says, "to my knowledge there wasn't ever any configuration done, or at least configuration that we knew of. Again, Cypress maintained that, so they may have had some configuration that I don't know about."[46]

Clearly Kaloustian did not configure the firewall, and admittedly had no knowledge of the firewall configuration. However it is his testimony upon which Ms. Hill relies to formulate opinions about the configuration of LabMD's firewall. **In fact, the default configuration of the ZyWALL 5 IPSec firewall *did prevent unauthorized traffic from entering the network***, and the Cisco 1841 likely did so in a redundant fashion as well.

Ms. Hill goes on to mistakenly conflate two different types of shared folders. In her discussion, she warns of the risks of using shared folders on an internal network for document sharing. She then claims "file-sharing applications, like LimeWire, also present the contents of shared folders to other users of those applications as information that is available to be downloaded."[47] That statement is simply incorrect. LimeWire shared folders are completely independent of the shared folders at the local network and Windows operating system level that Ms. Hill is referring to. A user can proactively choose to make available for sharing folder using LimeWire, but those shared folders have no relationship whatsoever to shared folders on the local network using Windows

[45] Kaloustian Dep. at 101.
[46] Kaloustian Dep. 97.
[47] Hill, Expert Report, at 43.

shared folders.

Ms. Hill further goes on to describe how support for SSL 2.0 on LabMD's servers presented significant network vulnerability. While the deprecation and vulnerability of SSL 2.0 is undisputed, it is important to note that at least two of the most popular servers on the Internet -- Integrated Information Services ("IIS") and Apache[48] – only disabled SSL 2.0 by default within the last two years, after the Relevant Time Period.[49] IIS 6.0, the version used at LabMD, shipped with SSL 2.0 enabled by default, but so did IIS 7.0, the version Ms. Hill recommends LabMD should have upgraded to as a means of addressing the problem. Furthermore, a casual scan of the top web sites on the Internet quickly reveals that the fourth most trafficked web site, yahoo.com, also supports SSL 2.0.[50]

While Ms. Hill is clearly correct that deploying File Integrity Monitors such as Nessus could have detected the presence of LimeWire on the network, they only could have done so with the necessary plugins configured especially for LimeWire detection.[51] Furthermore, Nessus would simply have been a more efficient means of performing the manual checks already in place at LabMD. File Integrity Monitors are also not listed in any of the available guidance for small businesses attempting to secure their networks. The Federal Communication Commission (FCC)'s "10 Cyber Security Tips for Small

---

[48] Apache Hause, Apache 2.2 Change Log, http://www.apachehaus.com/index.php?option=com_content&view=article&id=85:changelog-apache2&catid=41:catagory-change-logs&Itemid=88.

[49] Microsoft, How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services, http://support.microsoft.com/default.aspx?scid=kb;EN-US;187498.

[50] This is trivially verifiable through running the following command from any computer with openssl installed, such as an OSX or Linux computer: openssl s_client -ssl2 -connect yahoo.com:443

[51] Tenable Network Security, LimeWire Detection, http://www.tenable.com/plugins/index.php?view=single&id=11427.

Businesses," for example, states in recommendation #2 that companies simply do the following:

> Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.[52]

Similarly, the Internet Security Alliance makes no reference to File Integrity Monitors in their "Common Sense Guide to Cyber Security for Small Businesses."[53] Finally, NIST makes no mention of File Integrity Monitors in their 2009 guide, "Small Business Information Security: The Fundamentals."[54] Ms. Hill nevertheless cites all three references in her report.

Conclusion

While the Federal Trade Commission (FTC) is justified in attempting to maintain high standards for information security with regard to sensitive personal information of consumers, it is my opinion that during the Relevant Time Period LabMD did, in fact, adhere to reasonable standards to secure the Protected Health Information it possessed. Much of the FTC's expert analysis rests on a fundamental misunderstanding of peer-to-

[52] Federal Communications Commission, Cyber Security for Small Businesses, http://www.fcc.gov/cyberforsmallbiz.
[53] Internet Security Alliance, Common Sense Guide Cyber Security for Small Businesses, March 2004, available at: http://www.isalliance.org/publications/3C.%20Common%20Sense%20Guide%20for%20Small%20Businesses%20-%20ISA%202004.pdf.
[54] Richard Kissel, *Small Business Information Security: The Fundamentals*, October 2009, available at: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

peer networks and particularly LimeWire. That misunderstanding led to the faulty conclusion that LabMD's network security was inadequate.

In fact, LabMD's network adhered to best practices during the Relevant Time Period. It had two layers of firewalls protecting the network, and there is no evidence those firewalls were misconfigured. LabMD implemented proper user profiles on employee computers that limited the ability of non-managers to download files from the Interuet and to install applications. The Cisco 1841 deployed at LabMD was equipped with not only firewall capabilities but also had intrusion prevention capabilities, in fact exceeding the best practices outlined in the FTC's own recommendations. The ZyWALL 5 IPSec firewall offered an additional redundant layer of protection that shielded the LabMD network from unauthorized intrusion. Furthermore, LabMD outsourced its information technology infrastructure to two firms with the knowledge and expertise to deploy a secure network in Cypress Communications, Inc. and APT, and there is no evidence that those firms did not deploy secure networks using best practices.

Furthermore, while LabMD's IIS server did allow the deprecated SSL 2.0 protocol, that was the default IIS configuration in the version they used and in all subsequent IIS versions within the Relevant Time Period. While the LabMD network did not deploy File Integrity Monitoring, it did have a policy against installing applications that were unnecessary for performing work duties and performed regular checks on employee machines in an effort to ensure that employees adhered to that policy. The best practices guidelines reviewed for this report also did not include File Integrity Monitoring in their recommendations during the Relevant Time Period.

There is no evidence that LabMD's firewalls were, in fact, misconfigured, and they in fact had redundant firewalls protecting their network more than adequately. A similar employee action at the vast majority of small companies during the Relevant Time Period could have resulted in a disclosure of sensitive personal data despite **adequate** network security.

Ultimately it is my opinion that LabMD's security was reasonable and adequate to protect the PHI it possessed during the Relevant Time Period.

Dated: April 1, 2014

Adam Fisk

Appendix A: CV

Adam Archer Fisk

3615 Tacoma Ave, Los Angeles, CA 90038 • (917) 753-0673 • a@getlantern.org

Summary of Qualifications

Expert in peer-to-peer technology and computer networking and builder of peer-to-peer applications LimeWire, LittleShoot, and Lantern. One of the primary implementers of the US State Department's global Internet freedom initiatives.

Professional Experience

President, Founder, and Lead Architect **2010 – Present**
Brave New Software Project, Inc, Los Angeles, CA

Brave New Software is dedicated to building software tools to solve the world's toughest challenges. Its first product, "Lantern," is a secure, peer-to-peer-based censorship circumvention tool that uses a trust network. Deployed around the world and particularly popular in China and Iran, Lantern is funded through a $2.2 million dollar United States State Department grant. Brave New Software is also collaborating with Google to build next-generation censorship circumvention software.

President, Co-Founder, and Lead Architect **2004 - 2010**
LittleShoot, Los Angeles, CA

Managed all aspects of the company and led all programming for LittleShoot, the open source "P2P Browser Plugin." LittleShoot is the first true BitTorrent browser plugin ever made and incorporates multi-source downloading, NAT/firewall traversal, and video streaming. LittleShoot is also a reusable peer-to-peer library used by companies around the world. Companies can integrate LittleShoot directly at the code level or through an HTTP API that talks directly to the client.

Lead Engineer **2000 - 2004**
Lime Wire LLC, New York, NY

Led the engineering effort at LimeWire, the most widely used P2P application ever built in terms of raw numbers of users. Developed advanced search protocols and wrote all of the specifications

for how the major Gnutella programs implement search. This involved optimizing network topologies, adding new network messages, and creating new distributed algorithms.

Pioneered advanced downloading protocols that extended HTTP according to specifications standardized at LimeWire. These extensions form a "download mesh" using multi-source downloading similar to BitTorrent, but implemented long before BitTorrent existed.

Professional Affiliations

Sits on the Technical Advisory Committee of the Open Internet Tools Project, serves as technical and security advisor to the Human Interface Initiative in Auckland, New Zealand as well as to Tratado de Libre Comercio, LLC in New York, NY. Participant in the Internet Engineering Task Force (IETF) and speaker at events around the world, including the Nantucket Project, TEDx, and tech@state at the United States State Department.

Education

Brown University, Providence RI

B.A in Computer Science and U.S. History with honors.

Appendix B: Materials Considered or Relied Upon

Deposition Transcripts and Exhibits

05/23/2013 Kaloustian, Curt
11/21/2013 Boback, Robert Tiversa Rule 3.33
12/02/2013 Dooley, Jeremy
12/13/2013 Hyer, Robert
01/10/2014 Bureau, Matt
01/11/2014 Brown, Sandra
01/13/2014 Hudson, Lawrence
01/28/2014 Boyle, John
01/31/2014 Sandrev, Peter Cypress Communication Rule 3.33
02/05/2014 Simmons, Alison
02/07/2014 Gilbreth, Patricia
02/10/2014 Daugherty, Michael
02/11/2014 Parr, Jennifer
02/14/2014 Bradley, Brandon
02/27/2014 Truett, Allen
04/03/2014 Daugherty, Michael LabMD Rule 3.33

Correspondence	Bates Range
02/24/2010 Ellis Letter	FTC-LABMD-002506-FTC-LABMD-002520
06/04/2010 Ellis Letter	FTC-LABMD-002523-FTC-LABMD-002524
07/16/2010 Ellis Letter	FTC-LABMD-002495-FTC-LABMD-002503
07/16/2010 Ellis Exhibits	FTC-LABMD-002505-FTC-LABMD-003131
08/30/2010 Ellis Letter	FTC-LABMD-003132-FTC-LABMD-003137
08/30/2010 Ellis Exhibits	FTC-LABMD-003138-FTC-LABMD-003270
05/16/2011 Rosenfeld Letter	FTC-LABMD-003445-FTC-LABMD-003452
05/16/2011 Rosenfeld Exhibits	FTC-LABMD-003453-FTC-LABMD-003628
05/31/2011 Rosenfeld Letter	FTC-LABMD-003629-FTC-LABMD-003634
05/31/2011 Rosenfeld Exhibits	FTC-LABMD-003635-FTC-LABMD-003748
07/22/2011 Rosenfeld Email	FTC-LABMD-003749-FTC-LABMD-003750
07/22/2011 Rosenfeld Email	FTC-LABMD-003756-FTC-LABMD-003756

EXHIBIT 35

STAFF REPORT

TIVERSA, INC.: WHITE KNIGHT OR HI-TECH PROTECTION RACKET?

PREPARED FOR
CHAIRMAN DARRELL E. ISSA
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
JANUARY 2, 2015

EMBARGOED UNTIL AFTER THE TESTIMONY OF RICHARD WALLACE

Table of Contents

I. *Introduction* 5

II. *Tiversa's Scheme to Defraud the Congress and Executive Agencies* 6

III. *Tiversa's Lack of Cooperation with this Investigation* 7

IV. *Tiversa, Inc.* 9

A. Background on the company 9

B. Tiversa's claimed abilities to monitor and track files and users on the peer-to-peer network are exaggerated. 11

C. The Marine One leak 16

D. Boback created a hostile work environment at Tiversa 18

E. Boback has not been forthcoming regarding the nature of his close relationship with Wallace, or the central role Wallace played at Tiversa 26

F. Tiversa's Unseemly Business Practices 39

1. Tiversa used fearmongering tactics to generate business 39

2. Tiversa systematically mined for files for "potential" clients as a solicitation tactic. 42

3. Boback Misrepresented Howard Schmidt's Role in Generating Business Contacts for Tiversa 47

4. Boback Misrepresented Information about Tiversa's Capabilities to Clients 52

V. Tiversa's Relationship with the Federal Trade Commission 53

A. Tiversa misrepresented the extent of its relationship with the FTC to the Committee .. 54

B. The FTC misrepresented the extent of its relationship with Tiversa to the Committee. 56

C. The FTC failed to question Tiversa's creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC 58

D. Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit 62

E. Information provided by Tiversa formed the basis of the FTC's case against LabMD. 67

F. Tiversa withheld documents from the FTC 72

VI. *Tiversa's Involvement with House Ethics Committee Report Leak* 78

A. The *Washington Post* breaks the story 78

B. Tiversa "assists" the House Ethics Committee in its investigation 83

VII. *Open Door Clinic* 88

A. Initial contact with Tiversa 89

B. Tiversa only provided self-serving information to the Open Door Clinic in July 2008 92

C. Tiversa facilitates a class action lawsuit against the Open Door Clinic, and contacts Open Door patients directly 93

D. Tiversa did not charge Bruzzese for the same information it refused to provide to the Open Door Clinic 97

E. Tiversa provided information on the Open Door Clinic to the FTC 98

VII. *Conclusion* 98

Key Findings

- Rather than the cyber "white knight" Tiversa purports to be, the company often acted unethically and sometimes unlawfully in its use of documents unintentionally exposed on peer-to-peer networks.
- At least one Tiversa employee, under the direction of CEO Robert Boback, provided intentionally false information to the United States government on more than one occasion. Boback later provided false testimony about fabricated documents to the U.S. House of Representatives.
- According to a whistleblower, Tiversa fabricated that an Iranian IP address downloaded and disclosed the blue prints for the President's helicopter, Marine One. Tiversa allegedly did so in order to receive press attention for the company. The Committee found that statements made by Tiversa under oath about this matter could not be substantiated.
- After obtaining information on HIV/AIDS patients at a clinic in Chicago, Tiversa employees called the patients, purportedly in an attempt to get the clinic to hire Tiversa. When the clinic refused to hire Tiversa, the company gave the information to a lawyer that worked with the company who filed a class-action lawsuit that eventually settled for a substantial amount of money.
- Tiversa had information about a breach at the House Ethics Committee exposing information about investigations into Members of Congress. Tiversa did not return this information to the Ethics Committee and instead appears to have sought publicity for the leak.
- Tiversa's co-founder claims the company is in possession of a greater quantity of sensitive and classified information than NSA-leaker Edward Snowden.
- Information provided by Tiversa to the FTC through a shell organization known as the Privacy Institute was only nominally verified but was nonetheless relied on by the FTC for enforcement actions.
- Tiversa obtained non-public, advanced knowledge of FTC enforcement actions from which it attempted to profit.
- According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography and classified government documents.

I. *Introduction*

In the summer of 2013, the Committee learned the Federal Trade Commission would bring an enforcement action against LabMD, a Georgia-based cancer screening company, under the guise of its authority under Section 5 of the FTC Act.[1] Serving as the basis for the enforcement action, the FTC filed an administrative complaint against LabMD after the personal information of approximately 9,000 LabMD patients was exposed on a peer-to-peer network.

Tiversa, a Pittsburgh-based company that sells peer-to-peer monitoring services, provided information on LabMD and nearly 100 other companies to the FTC. This information formed the basis for multiple enforcement actions and dozens of warning letters sent by the FTC. In August 2013, Mike Daugherty, LabMD's CEO, expressed concern to the Committee about both the relationship between the FTC and Tiversa, Inc., and the veracity of the information provided by Tiversa. In April of the following year, the Committee became aware of a former Tiversa employee with allegations of substantial misconduct related to Tiversa's dealings with the federal government.

Committee staff interviewed Tiversa's CEO, Robert Boback, on June 5, 2014. Boback's testimony failed to assuage Committee's concerns and instead raised many more questions about the relationship between Tiversa and various federal government agencies. Two days later, Boback was deposed for a second time in the FTC action against LabMD. There were several major inconsistencies between this testimony and the testimony he provided to the Committee only days earlier.[2]

During the course of this investigation, the Committee conducted ten day-long transcribed interviews and reviewed over 50,000 pages of documents. Documents and testimony obtained by the Committee in the course of its investigation displayed a troubling pattern with respect to Tiversa's business practices. Tiversa routinely provided falsified information to federal government agencies. Instead of acting as the "white knight" the company purports to be, Tiversa often acted unethically and sometimes unlawfully after downloading documents unintentionally exposed on peer-to-peer networks. At least one Tiversa employee, under the direction of Boback, provided intentionally false information to the United States government on more than one occasion. This is a crime. In addition, Boback provided false testimony about fabricated documents to the U.S. House of Representatives.

In many instances, documents that Tiversa produced to the Committee pursuant to a subpoena issued on June 3, 2014 lacked important context without explanation. Such gaps prompted the Committee to ask Tiversa's representatives on several occasions whether the company had produced all documents responsive to the Committee's subpoena as well as search terms proposed by Committee staff. Tiversa did not provide the Committee with assurances or a written statement that all documents had, in fact, been produced. Accordingly, the Committee sought to obtain additional information from third parties. These third parties provided a substantial number of documents to the Committee that Tiversa failed to produce. For example, Tiversa never produced documents showing it had advanced non-public knowledge of FTC

[1] Federal Trade Commission Act, 15 U.S.C. § 45 (2006).
[2] The Committee sent Boback a lengthy letter demanding explanations for the inconsistencies. Many questions posed in that letter remain unanswered.

enforcement actions and took steps to profit from that knowledge. The Committee also found that Tiversa withheld from the FTC a series of documents that are inconsistent with testimony company officials provided under oath. Tiversa's lack of cooperation with this investigation, and the withholding of key documents from the FTC, lead the Committee to believe that Tiversa has not produced all relevant documents responsive to this Committee's subpoena.

According to the testimony of a whistleblower and documents obtained in this investigation, Tiversa appears to have provided intentionally false information to this Committee and numerous other federal departments and agencies. Tiversa has further used and overstated its relationships with Congress and federal agencies to advance its unethical business model. The Committee's findings should give pause to any government entities which have relied or are planning to rely on information provided by Tiversa.

II. *Tiversa's Scheme to Defraud the Congress and Executive Agencies*

Several years ago, Tiversa CEO Robert Boback began perpetrating a scheme in which at least one Tiversa employee manipulated documents legitimately found on the peer-to-peer network to show that the documents had spread throughout the peer-to-peer network. For example, Tiversa downloaded a file that computer A shared on a peer-to-peer network. The file could be copied and the metadata easily manipulated thoroughly widely-accessible computer software programs to make it appear that it had been downloaded by computers B, C, and D, and thus spread throughout the peer-to-peer network. Tiversa relied on the manipulated documents to create a need for their "remediation" services and to grow the company's reputation through press statements and manipulation of media contacts. Boback told media contacts that certain documents, including sensitive government documents, spread throughout the peer-to-peer network when in fact they had not.

According to a whistleblower, Tiversa not only provided the manipulated information to its clients, but in some instances also provided false documents to various entities of the United States government, including the Congress and several agencies. Not only is this unethical, but it is illegal to give false information to the United States government.[3] It is also illegal to obstruct a congressional investigation by providing false information to a congressional committee.[4]

---

[3] See 18 U.S.C. § 1001, which states in pertinent part:

> [W]hoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully . . . makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry shall be fined under this title, imprisoned not more than 5 years. . . .

[4] See 18 U.S.C. § 1505, which states in pertinent part: 18 U.S.C. § 1505 states, in pertinent part:

> Whoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States, or the due and proper exercise of the power of inquiry under which any inquiry or investigation is being had by either House, or any committee of either House or any joint committee of the Congress—

Throughout this investigation, the Committee routinely found that information provided by Tiversa either could not be verified, or simply did not make sense. Part of the story always seemed to be missing. The whistleblower's testimony that Tiversa routinely falsified documents, however, filled in these gaps.

III. *Tiversa's Lack of Cooperation with this Investigation*

Over the course of this investigation, Tiversa failed to provide full and complete information to the Committee. On multiple occasions, the company received documents from third parties witnesses responsive to the Committee's subpoena and other document requests, but not produced by Tiversa.

The Committee issued a subpoena to Tiversa on June 3, 2014. The subpoena requested documents responsive to eleven different requests, including:

1. All documents and communications referring or relating to work performed by Tiversa, Inc. on behalf of, in conjunction with, or provided to, any department, agency, or other instrumentality of the U.S. Government.

2. All documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission.

* * *

4. All documents and communications referring or relating to internet protocol addresses that Tiversa, Inc. provided to any department or agency of the U.S. Government.

* * *

7. All documents and communications referring or relationg to LabMD, Inc.[5]

Tiversa failed to fully comply with the subpoena. A third-party witness provided numerous documents to the Committee in which Tiversa discussed information it provided to the FTC, and knowledge it had of upcoming FTC enforcement actions, with that third-party. Tiversa failed to produce these documents to the Committee despite their clear responsiveness to the subpoena.

Tiversa withheld additional relevant documents responsive to subpoenas issued by the Committee and the FTC from both entities. In October 2014, Tiversa filed a Notice of

---

Shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331), imprisoned not more than 8 years, or both.

[5] H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014) [hereinafter Tiversa OGR subpoena].

Information in the LabMD FTC proceeding.[6] Tiversa included two e-mails from 2012 as exhibits to the Notice of Information, claiming that the e-mails demonstrate that Wallace could not have fabricated the IP addresses in question. Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission to the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. Tiversa has not explained how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information supporting their position that the documents undermine what they assume to be Wallace's testimony.

Tiversa further failed to fully respond to a subpoena issued by the Federal Trade Commission. As discussed in more detail below, the FTC served Tiversa with a subpoena for documents related to its administration action against LabMD, a Georgia-based medical testing laboratory.[7] Among other categories of documents, the subpoena requested "all documents related to LabMD."[8] In responding to the subpoena, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Finally, after the Committee learned of Tiversa's involvement with the Open Door Clinic, an AIDS clinic servicing low-income patients outside of Chicago, Tiversa produced selected documents about its involvement with the Open Door Clinic. Committee staff requested specific additional information, including any forensic analysis done by Tiversa of the Open Door Clinic files. Tiversa, through its attorneys, told the Committee that it only analyzed one of the numerous files that it found on the peer-to-peer network about the Open Door Clinic.[9] In fact, as discussed below Tiversa provided extensive forensic services, including two versions of a forensic report, free of charge to Michael Bruzzese. Bruzzese filed a lawsuit against the Open Door Clinic after receiving information from Tiversa. Tiversa never produced the reports to the Committee. Tiversa's withholding of these reports in the face of a direct request from the Committee, and its false claim that it did not analyze most of the Open Door files, is unacceptable.

Given these numerous instances in which Tiversa failed to fully provide information to the Committee and the FTC, the Committee strongly believes that Tiversa may be withholding additional relevant documents. Tiversa's failure to produce numerous relevant documents to this Committee and the FTC, at a minimum, demonstrates a lack of good faith. At worst, Tiversa intentionally withheld documents and other information in the face of multiple subpoenas. Either way, Tiversa's actions call into question the credibility of the company and its CEO, Robert Boback, as a source of information for the FTC.

---

[6] Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014) [hereinafter Notice of Information]. Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose." Order on Respondent's Motion to Strike, In the Matter of Lab MD, Inc., No. 9357 (Nov. 19, 2014).
[7] Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC subpoena].
[8] *Id.*
[9] Letter from Reginald J. Brown and Madhu Chugh, Wilmer Hale, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2014).

Boback created a culture of intimidation at Tiversa. The Committee has unfortunately learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.[10] Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. The suit against Wallace effectively questions Mr. Wallace's Constitutional right to speak with Congress after the Committee approached him with questions related to allegations about Tiversa. These are clear instances of witness intimidation and interference with a congressional investigation on the part of Boback and Tiversa.

IV. *Tiversa, Inc.*

A. Background on the company

Robert "Bob" Boback and Samuel Hopkins founded and incorporated Tiversa, Inc., a privately-held corporation headquartered in Pittsburgh, Pennsylvania, in January 2004.[11] Prior to joining Tiversa, Boback was a practicing chiropractor who dabbled in other activities including buying and selling residential properties and selling cars on eBay.[12] Hopkins, a high-school dropout, wrote the source code for the proprietary technology that Tiversa later patented.[13] Hopkins sold his shares in Tiversa for approximately $3.5 million and left the company in 2011.[14] Boback is currently the Chief Executive Officer.[15]

Tiversa promotes itself as a company of "cyberintelligence experts."[16] The company maintains an impressive roster of Advisory Board members, including retired General Wesley Clark; Howard Schmidt, the former Cyber-Security Coordinator for President Obama and previously for President Bush; and Maynard Webb, the former CEO of eBay.[17] The Advisory Board met on one occasion in January 2006.[18]

According to Tiversa's website, the company "provides P2P Intelligence services to corporations, government agencies and individuals based on patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day. Requiring no software or

[10] E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).
[11] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback (June 5, 2014), at 7 [hereinafter Boback Tr.].
[12] *Id.* at 7.
[13] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Samuel Hopkins (July 29, 2014), at 115, 56 [hereinafter Hopkins Tr.]; Boback Tr. at 56.
[14] *Id.* at 8.
[15] Boback Tr., at 8.
[16] Tiversa, Company Overview, http://www.tiversa.com/about/ (last visited Sept. 15, 2014).
[17] *Id.*
[18] Boback Tr. at 29.

hardware, Tiversa can locate exposed files, provide copies, determine file sources and assist in remediation and risk mitigation."[19]

On July 24, 2007, during the tenure of Chairman Henry Waxman, Boback testified at a hearing before this Committee titled, "Inadvertent File Sharing Over Peer-to-Peer Networks."[20] Boback's 2007 testimony focused on the "privacy and security threats [that] are caused by inadvertent misuse of P2P file sharing software," and his company's work in this area.[21] On July 29, 2009, when Rep. Edolphus Towns served as Committee Chairman, Boback again testified about Tiversa's work in the area of P2P filing sharing and data security breaches.[22] One particular statement garnered a great deal of attention from Members of the Committee and the national media. Boback testified:

> In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.[23]

During this hearing, Boback also provided information on files Tiversa obtained from numerous other companies and non-profit groups, including the Open Door Clinic that Tiversa had "discovered" on the peer-to-peer network.[24]

According to a customer presentation document, Tiversa began working with U.S. government in the spring of 2004. Tiversa claims to have worked "exclusively with the CIA, DoD, DHS, FBI, JCS, and USAF regarding the disclosure of CLASSIFIED [*sic*] information."[25] In reality, Tiversa may not have worked with some of these agencies at all. With others, its relationships were extremely minimal. Overall, the company's claims are overstated.

From 2008 to 2009, Tiversa frequently contacted non-client companies whose documents it discovered on peer-to-peer networks. Under a "duty of care" policy, Tiversa notified companies whose information they found on peer-to-peer networks, and provided them with examples of the exposed documents.[26] Boback explained that by providing this information, Tiversa was essentially providing a public service. In practice, however, Tiversa provided very minimal information to the affected companies. The Committee's investigation found that Tiversa typically provided one document. Even though Tiversa's systems automatically captured other relevant information, such as the IP address from which the

---

[19] *Id*.
[20] Peer-to-peer networks are often referred to as "P2P" networks.
[21] *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov't Reform*, 110th Cong. (2007) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).
[22] *Inadvertent File Sharing Over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security*, 111th Cong. (2009) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.).
[23] *Id*.
[24] *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. at 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.).
[25] [TIVERSA-OGR-0021275].
[26] Hopkins Tr.,at 205-06.

document was shared, Tiversa would not provide this information to a company unless it purchased Tiversa's services.

During the course of this investigation, the Committee spoke with several companies that chose not to hire Tiversa. In addition, the Committee located one company that did enter into a contract with Tiversa. Tiversa told the company that it spent a great deal of time "investigating" the source of the peer-to-peer leak, at high cost to the company. It appears, however, that Tiversa only provided information its systems automatically downloaded, such as the IP address that leaked the documents.[27] Tiversa further represented to this company that, in order to identify whether any of its computers had peer-to-peer software, it would have to access the company's network remotely and run a search. Tiversa lacks the capability to access a client's network remotely. In this instance, it seems likely that it "identified" the computer using peer-to-peer software by simply looking at the IP address of the computer that shared the confidential document. When the Committee asked Tiversa about its ability to remotely access client computer, Tiversa responded that it never made such a claim to any client.[28]

In his transcribed interview, Samuel Hopkins described Tiversa as "a highly ethical company."[29] After a lengthy investigation, the Committee believes otherwise.

B. Tiversa's claimed abilities to monitor and track files and users on the peer-to-peer network are exaggerated.

Tiversa's business model relies on technology developed by Hopkins, including its trademarked and patented Eagle Vision X1 and Covio. Tiversa claims to have the ability to provide "true cloud security" by seeing the entire peer-to-peer network."[30] Further, Tiversa states that its technologies can "detect and record user-issued P2P searches, access and download files available on the P2P networks, determine the actual disclosure source of documents, track the spread of files across the entire P2P networks [*sic*], and remediate P2P file disclosures."[31]

Tiversa claims that its technology "enables us to view the entire network and thus provide real-time, actionable information regarding sensitive file disclosures related to your organization."[32] In 2007, Boback's written testimony submitted to the House Oversight Committee summarized Tiversa's technological capabilities. Boback wrote:

> Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, **Tiversa can see the P2P network in its entirety in real time.**

[27] Briefing by Company A to H. Comm. on Oversight & Govt' Reform (July 16, 2014).
[28] Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 2, 2014).
[29] Hopkins Tr.at 54.
[30] Tiversa Learning Ctr., *Key Concepts*, http://www.tiversa.com/learningcenter/resources/keyconcepts/.
[31] Marine One forensic report, pg. 2.
[32] Tiversa Learning Ctr., *FAQ/Misconsceptions*, http://www.tiversa.com/learningcenter/resources/faq/.

> With this platform, **Tiversa has processed as many as 1.6 billion P2P searches per day**, more than the number of web searches entered into Google per day.[33]

It is disputed, however, how many files Tiversa downloads daily off the peer-to-peer network. According to Jason Schuck, Tiversa downloads "maybe a million" files daily.[34] However, according to Boback, Tiversa downloads "the equivalent of the Library of Congress every three or four days."[35] The Library of Congress is the largest library in the world, with more than 158 million items, including more than 36 million books and other print materials, 3.5 million recordings, 13.7 million photographs, 5.5 milion maps, 6.7 million pieces of sheet music, and 69 million manuscripts.[36] In essence, Tiversa claims to be able to see the entire peer-to-peer network, instead of a smaller subset as seen by an individual user.

At the time of the leaks discussed in this report, Tiversa used generic and client-specific search terms, such as "reports," "credit card," or "secrets" to query the peer-to-peer network.[37] Even Tiversa analysts could not explain exactly how Eagle Vision keyed into the terms to download them into the data store; that is, analysts did not know definitively whether any document was in the data store due a search term hitting on the file's name, for instance; the search term in the body of the file; or the search term in the name of a folder containing the file. Keith Tagliaferri, Tiversa's Senior Vice President of Operations, and the individual in charge of Tiversa's analytical work, stated:

> I'm not well versed enough on the technology and how it works to know exactly how things key off and what could have downloaded this and that.
>
> I'm aware of all different types of scenarios that can happen as far as why and when we download files. You know, one is matching a key term within a file title. Another is matching a key term within the content of a file.
>
> I've read research that indicates that a folder name can hit on a file. So, for example, if you have a folder called "Work" and somebody searches for "Work," the results that come back are all of the files that are within that folder.
>
> There's also a concept of browse host on peer-to-peer that I'm not sure if our systems have the ability to do or not. But you can literally go to an IP once you find one file and hit "Browse Host" and download all the files from that IP.

---

[33] *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov't Reform*, 110th Cong., at 20 (2007) (written statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.) (emphasis added)
[34] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jason Schuck, at 12 (Aug. 1, 2014) [hereinafter Schuck Tr.]
[35] Boback Tr. at 143.
[36] Library of Congress, Fascinating Facts, http://www.loc.gov/about/fascinating-facts/ Fascinating Facts (last accessed Dec. 22, 2014).
[37] Hopkins Tr. at 74.

> So there's all kinds of different scenarios that can occur to cause files to be downloaded. I'm not well versed enough on the technical side of our systems to know exactly what would trigger files to be downloaded.[38]

To Tagliaferri's knowledge, there was no way to verify by what search term a document was found and downloaded into the data store.[39]

Tiversa's data store collects and accumulates all the information that is found by Eagle Vision; no documents are deleted.[40] Information enters Tiversa's data store, or repository of databases, in two ways. Either Tiversa's Eagle Vision software downloads the information from the peer-to-peer network, or the information is found independently from Eagle Vision and "injected" into the data store through an application called the Data Store Importer. Schuck described the application in the following way:

> Q. **So analysts have the ability to, I guess, inject files into the data store using the Data Store Importer program?**
>
> A. **Correct**. [41]
>
> * * *
>
> Q. How does it -- if I'm an analyst and I have a file that I want to put into the data store using this program, do you know what steps I take to do that?
>
> A. Sure. If the file is in the correct format, you would place it in a pickup folder.
>
> Q. What does it mean to have a file in the correct format?
>
> A. So depending on the IP address that it was downloaded from, that would be prepended to the original file name.
>
> Q. Who prepends the IP address?
>
> A. Again, you're talking about for the Data Store Importer, right?
>
> Q. Yes.
>
> A. That would be whoever's bringing it in.

[38] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of KeithTagliaferri, at 106-07 (June 17, 2014) [hereinafter Tagliaferri Tr.].
[39] *Id*. at 107.
[40] *Id*. at 88-89.
[41] Schuck Tr. at 19.

Q. Are you aware of specific occasions on which the data store importer was used by analysts to put files into the data store?

A. No, not offhand. That's, again, that's even though I oversee that, I'm not the one that's actually doing that. That would be the analyst.

Q. To your knowledge, has the Data Store Importer been used to put files into the data store?

A. I would assume so, yeah.[42]

Eagle Vision directly downloads documents that either directly hit on a Tiversa search term, or are related to a Tiversa search term (i.e., other documents shared by a user also sharing a document that hits on a search term).[43] According to Hopkins, the creator of the technology, the system does not distinguish between downloaded and injected files.[44] Tiversa, through its attorneys, stated that analysts can "usually" tell if a file is downloaded or injected, but did not explain how its analysts can make that determination.[45] This distinction is critically important, as it would aid in understanding more fully Tiversa's actions.

Tiversa's Covio system indexes the IP address of all files it downloads from the peer-to-peer network. Every time a document containing a search term is shared on the peer-to-peer network, Tiversa's system downloads the document and indexes it according to the IP address from which it was downloaded. Even if the document is exactly the same, the system will automatically re-download it and index it with the new IP address.[46] In this way, Tiversa can determine if a file is spreading, or being shared, throughout the peer-to-peer network.

Boback, however, has offered the Committee conflicting information about whether Tiversa's technology actually does have the capability to automatically download and index documents as they spread throughout the peer-to-peer network. For example, according to Boback, Tiversa never downloaded a copy of a document belonging to LabMD, a cancer screening company, from one of LabMD's computers in Georgia.[47] This document is at the heart of an ongoing FTC action against LabMD. Yet, the document hit on a search term provided by a client, and Tiversa does claim to have downloaded the file from several other IP addresses because of the search term.[48] Tiversa has never been able to explain to this Committee why its systems did not automaticallydownload the file from LabMD but did download the document from so many other IP addresses. Either Tiversa's technology can not do what Boback and Hopkins claim it can do, or Boback provided false information to the FTC and this Committee about Tiversa's downloading of the LabMD document.

---

[42] Schuck Tr. at 20-21.
[43] Hopkins Tr. at 43.
[44] *Id.* at 75.
[45] Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Sept. 2, 2014).
[46] Hopkins Tr. at 40.
[47] *Id.*; *see also* Tiversa, Forensic Investigation Report – LABMD0001 (June 4, 2014).
[48] Boback Nov. 2013 FTC Tr. at 41 ("I never downloaded the file from them. They only responded to the hash match.").

Further, Tiversa has not taken steps to screen for illegal content, such as child pornography, before it is downloaded into the data store. In fact, analysts say that it is entirely possible that child pornography is sitting in Tiversa's data store currently. According to a whistleblower, Tiversa has knowingly accumulated and is in possession of massive amounts of child pornography. Tagliaferri stated that he had "heard anecdotally that there may be child pornography" downloaded into the data store.[49] He explained that "as part of that information that's being pulled down, you know, I suppose anything -- anything could come back. You know, it could be Word documents. It could be .pdf's. It could be images. It could be, you know, whatever."[50]

According to Tiversa, The system also "records all user-issued P2P searches," meaning that Tiversa can see a search and record it.[51] Typically, Tiversa can only see the queried search, and cannot identify the user issuing the search. Under very narrow circumstances, Tiversa can determine the IP address of the user issuing a search. Hopkins described Tiversa's limited ability to identify the IP address issuing a search. He stated:

> [The search request] goes to the first three people, they hand it to all the three people there, so it's three and then it's what, nine, so forth. But it only goes five hops. So the three people that I'm connected to, that's the first hop. . . . After five hops, it's dropped off the network. But if you're connected to the three people and the search is one hop away, then you know it came from one of the people you're connected to. But out of the 3,000 people, three people in a security world is nothing.[52]

Thus Tiversa can only determine the IP address of a user issuing the search if Tiversa is one of the three users directly connected to the searcher.

Boback, however, has exaggerated Tiversa's ability to determine the user issuing a search over the years. In 2011, Tiversa claimed to have information that Wikileaks was obtaining information from peer-to-peer networks.[53] Boback claimed that "Wikileaks is doing searches themselves on file-sharing networks."[54] He continued, "It would be highly unlikely that someone else from Sweeden is issuing those same types of searches resulting in that same type of information."[55] Boback further explained that in a one-hour period in February 2009, Tiversa detected four Swedish computers issue 413 searches.[56]

As explained to the Committee by Hopkins, however, Tiversa can only identify the IP address and geographic location of a computer issuing a search if Tiversa is one of only three peer-to-peer users directly connected to that computer. Otherwise, Tiversa can only see the search request, and not the user or location of the user issuing the search. Given the limitations of Tiversa's technology, Boback's statements are very likely exaggerated, if not outright false.

---

[49] Tagliaferri Tr. at 90.
[50] *Id.* at 91.
[51] *Id.* at 160.
[52] *Id.* at 169.
[53] Michael Riley, *Wikileaks May have Exploited Music, Photo Networks to Get Data*, BLOOMBERG (Jan. 20, 2011) http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html.
[54] *Id.*
[55] *Id.*
[56] *Id.*

Tiversa also claims that it can "remediate" damage from a document leaked over the peer-to-peer network. Tiversa, however, cannot remove an exposed document from the peer-to-peer network. Instead, Tiversa is limited to sending take-down notices to the internet service provider of the IP address. The success of the take-down notices depends, in part, on the location of the ISP.[57]

C. The Marine One leak

In early 2009, Tiversa's reputation exploded when the company disclosed that it found blueprints for Marine One on a computer in Iran. A whistleblower stated to the Committee, however, that Tiversa only found on the blueprints on a government contractor's computer. Tiversa then manipulated the document by prepinning an Iranian IP address to make it appear that the plans had been downloaded in Iran via the peer-to-peer network. At Tiversa's request, the Committee spoke with multiple federal agencies involved in the investigation into the Marine One leak. The Committee reviewed documents provided by Tiversa, including a forensic report prepared by Tiversa in June 2014, and received briefings and documents from federal agencies involved in the government's investigation of the leak.[58] The Committee found that statements made by Tiversa about the Marine One leak could not be substantiated.

On September 17, 2007, Tiversa "detected" the Marine One file as being shared on the peer-to-peer network. Tiversa's Eagle Vision software did not download this file automatically. Instead, a Tiversa analyst found the file using a stand-alone computer to search the peer-to-peer network. Tiversa determined that a government contractor was sharing the document on a peer-to-peer network.[59] That a contractor inadvertently shared the document on the peer-to-peer network is not in dispute. Tiversa, however, additionally claimed that a computer located in Iran downloaded and shared the file. These explosive allegations garnered large amounts of publicity for the company.

Tiversa claims that on February 25, 2009, it found that an Iranian computer was in possession of the same Marine One blueprints previously shared by the government contractor. According to Tiversa's forensic report, the Iranian computer disclosed the document on the peer-to-peer network between October 27, 2006 and February 25, 2009.[60] Thus, Tiversa conveniently found the document on the network the very last day it was made available by the Iranian computer. The fact that the Iranian computer ceased sharing the document made it next to impossible for any agencies Tiversa alerted after February 25 to determine whether that computer was in fact in possession of the Marine One file.[61]

---

[57] Tagliaferri Tr. at 120, 161.
[58] All information contained in this report was provided to the Committee in an open and unclassified setting.
[59] Forensic Report at 4.
[60] Forensic Report at 10.
[61] If the computer was still sharing the file after Tiversa reported its purported discovery, then individuals investigating the leak could have determined whether the document was, in fact, sharing the file using the peer-to-peer network.

The Committee spoke with Tim Hall, a former NCIS employee who investigated the Marine One leak, on multiple occasions. Hall is now the Director of Government Services at Tiversa.[62] Hall told the Committee that another federal agency verified the information provided by Tiversa about the Marine One leak—specifically, that another agency verified that the file was being shared by a computer with an Iranian IP address. Hall testified:

> Q. And do you know if the information was verified by other task force members?
>
> A. Yes.
>
> Q. How do you know that?
>
> A. Because we worked hand in hand with them daily, just multiple conversations.
>
> Q. Were you ever told how the information was verified?
>
> A. No.
>
> Q. Was all information passed on to other task force members to be verified, to the best of your recollection?
>
> A. Yes. Yes.[63]

Tiversa's counsel also repeatedly told the Committee that the federal government verified the information Tiversa provided about an Iranian computer being in possession of the Marine One document. But that is simply not the case. The Committee learned from NCIS that the joint task force investigating the incident was only able to verify that the IP address provided by Tiversa was located in Iran.[64] The agents did not verify whether that computer actually possessed the Marine One file as this was outside the scope of the investigation.[65]

Given the amount of time that has passed, it is not possible to verify today whether the Marine One file ever spread to a computer in Iran. The Committee has great doubts, however, about Tiversa's story. Tiversa discovering that the document had spread to Iran on the very last day that the Iranian computer allegedly disclosed the file is far too convenient. Further, the Iranian computer purportedly shared the computer for over two years before Tiversa located the file. According to Tiversa, the Iranian computer was in possession of the file in September 2007, when Tiversa initially found that a government contractor improperly shared the document. Yet, Tiversa did not locate the file on the Iranian IP address at that time.

---

[62] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Timothy Hall at 26 (Sept. 3, 2014) [hereinafter Hall Tr.].
[63] Hall Tr. at 25-26.
[64] Briefing by Naval Crim. Investigative Service to H. Comm. on Oversight & Gov't Reform Majority and Minority Staff (Sept. 5, 2014). In the course of the investigation, the Committee received a document from a Tiversa whistleblower listing hundreds of IP addresses in rogue nations around the world.
[65] *Id.*

Tiversa has also not been able to explain to the Committee how it finally learned in February 2009 that the file spread to the Iranian computer. A Tiversa analyst found the original file in 2007, meaning that either no word in the document hit on a Tiversa search term, or Eagle Vision did not download the document when it should have done so.[66] Given that Eagle Vision also did not download the document between September 2007 and February 2009, it would appear that no word in the document hit on a Tiversa search term.[67] So, what prompted Tiversa to search for the document again in late February 2009? That the document does not appear to have been downloaded by Eagle Vision makes the fact that Tiversa downloaded the document on the very last day it was shared by the Iranian computer even more fortuitous.

The story is complicated, to be sure. But Tiversa's complicated tale about this leak unwound when the Committee heard from a whistleblower. According to the whistleblower, Tiversa fabricated that the Iranian IP address downloaded and disclosed the Marine One file. Tiversa allegedly did so in order to receive press attention for the company. This is a very serious allegation—one outside the capabilities of the Committee to verify. If true, then Tiversa provided knowingly false information to numerous agents of the federal government, including this Committee, and wasted federal resources as numerous agencies investigated a fraudulent report. Additionally, the publicity associated with this breach allowed Tiversa to exaggerate the degree to which U.S. intelligence was vulnerable to P2P leaks and sell itself as the solution.

D. Boback created a hostile work environment at Tiversa

Not only does Boback appear to have routinely exaggerated the technological capabilities of Tiversa, but he also created a hostile work environment and retaliated against employees who questioned him. In fact, numerous witnesses put Boback at the center of a hostile work environment at Tiversa. One Tiversa employee stated that he "had significant concerns about [Boback's] ability to execute his job as CEO."[68] The employee brought his concerns to a board member, citing Boback's role in the "creation of a toxic environment," "certain bullying incidences," and "certain practices that I thought were reckless or inappropriate."[69] A faction of employees, led by Boback, frequently left work, offended other employees, and engaged in unprofessional behaviors, including carrying guns to work.

Boback left the office frequently, sometimes for multiple days. In one instance, in early 2008, Boback left with Richard Wallace, the Director of Special Projects at Tiversa, "to pick up

[66] As explained above in Section IV(B), Tiversa's technology should download a document containing a search term each time it spreads throughout the peer-to-peer network. Here, the Iranian computer downloading and sharing the document would create a new document in the eyes of the Eagle Vision system. If the document contained a search term, then it should have been downloaded. If the document contained a search term but was not downloaded for some reason, then Tiversa's software failed to operate as advertised.

[67] Given the magnitude of the discovery, the Committee does not understand why Tiversa would not input key terms from the Marine One document into its automatic download system. Given the gap in time between the discovery of the two documents, either Tiversa neglected to perform this basic task for a leak of great national security significance, or its systems failed to perform as advertised.

[68] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Christopher Gormley, at 27 (July 14, 2014) [hereinafter Gormley Tr.].

[69] *Id.* at 27.

a car in Atlanta."[70] They were scheduled to be gone for only a day, but were instead gone two days.[71] A former Tiversa employee said that this was a frequent habit: "Mr. Boback would generally come in late in the morning and leave fairly early in the afternoon as well... I'm not sure where he was during those hours."[72]

Boback encouraged imappropriate banter and comments by employees that detracted from the professional atmosphere and mission of Tiversa. One former employee testified:

> Q. I'd like to start with a little bit of follow-up from the last hour. You were discussing with my colleagues some joking emails, I guess, for lack of a better term, that Mr. Wallace sent, and I believe you described that there were many of these emails that were sent among a certain group of people. Is that accurate?
>
> A. I wouldn't say so much many emails, but there was a lot of banter, I guess, orally. And I'd say there was a certain amount of that you'd expect, but some of it in this case was out of line for what I considered a company of what we were trying to create was.
>
> Q. Was Mr. Boback ever involved in this banter?
>
> A. Yes.
>
> Q. Did he ever express that he felt the banter was not appropriate for the workplace?
>
> A. No.
>
> Q. Did he make joking comments along the same lines of what other employees were saying?
>
> A. Yes.[73]

Boback routinely made offensive remarks to Tiversa employees, creating an atmosphere of harassment and intimidation. One employee described described Boback's inappropriate comments to the Committee:

> A lot of, I guess, homosexual jokes, right? This or that. I mean, something akin to being in a junior high school playground, and it was fairly rampant, and it was just, you know, difficult to not engage in that… one particular story that I do remember is we had a company meeting. Well, I entered the company meeting, and one of the -- and I don't remember who -- made a remark to that effect, and everyone in the meeting laughed,

[70] *Id*. at 38.
[71] *Id*. at 38.
[72] *Id*. at 40.
[73] *Id*. at 79.

> including Mr. Boback. It was clearly uncomfortable for many in the room. And I think, you know, those are the issues I was trying to convey to the board member, just that we can't have an environment like that in today's day and age, and that can we at least put some boundaries to that kind of behavior inside the office.[74]

Gormley described another instance of Boback acting in an unprofessional manner :

> I remembered receiving an email that copied a colleague of mine, Griffin Schultz, that said, you know, "Chris, you should get a job as a Presidential piss boy," which just out of, you know -- stated very clearly it was a joke, but he stated it, that I should get that kind of job.[75]

* * *

> Q. What did you understand him to mean by that phrase?
>
> A. I don't know what was in Mr. Boback's mind when he made that, other than the email said what it said. The context was Mr. Schultz was trying to make an introduction to some congressional staffers or somebody that he had known in the past, and there may have been some mention of various roles, but not Presidential piss boy, but it may have been in the context of that. And then he said, Chris, that's a great job for you, Presidential piss boy, and Griffin Schultz was on that email as well me.
>
> Q. Do you recall when that email was sent?
>
> A. That would have been, I believe, April 2008. It was in 2008. I don't -- I think it's April.[76]

Boback also referred to "teabagging" with Wallace and Hopkins while at work. One employee described conversations he overheard at the office:

> I would be at my desk listening to them talk about playing Halo 3 and how they teabagged this person from Russia or this person from -- but it was extremely rampant to the point where it was very disruptive to the business. So that was one of the things I reported to the board member, to say we need to get them engaged back in the business, because, you know, they were needed for doing business, and I, again, didn't think that was an appropriate conversation for a work office.[77]

---

[74] *Id*. at 79-80.
[75] *Id*. at 19-21.
[76] *Id*. *at* 57-58.
[77] *Id*. at 179-80.

Boback also condoned employees carrying and wielding firearms , and brought a gun himself to the office on multiple occasions. Transcribed interviews with Tiversa employees reflect that both Sam Hopkins, the co-founder of Tiversa, and Boback carried guns while at work at Tiversa. Sam Hopkins was aware that Boback carried a gun around at the office:

> Q. Did you ever see any other weapons in the office of any kind?
>
> A. Bob had a handgun that I saw a few times.
>
> Q. And did he show you the gun when he was in the office?
>
> A. In his office, yeah.
>
> Q. Why did he -- do you know why he showed you this gun or do you–
>
> A. You know, just two guys talking and he had known that I was carrying.[78]

Keith Tagliaferri saw Boback "walk by with [a gun case]," although he did not look inside the case.[79] Christopher Gormley was also aware that Boback carried a gun at work. Boback even showed Gormley his gun:

> Q. And what was the context of the meeting at which Mr. Boback pulled out his revolver and showed it to you?
>
> A. He just came in. He'd come in a lot. I mean, his office was close to mine. And, I believe, that day -- and I can't be certain of this, but I'm pretty sure that he had taken a number of individuals from the company out to shop for guns at a gun store.
>
> Some people from the company actually departed for the afternoon, and I didn't know where they went. Which was a fairly common activity, that he would disappear for long periods of time. But this particular afternoon, I mean, that was my belief at the time, that they went to a gun store, and this may have been a purchase then. But it was showing me that he had purchased this or had this. I wasn't sure whether he actually got it at the gun store or not. But that activity occurred that day.
>
> Q. Do you recall approximately when this took place?
>
> A. Yes. Well, let me think. It would've been in the first quarter of 2008, maybe April.[80]

[78] Hopkins Tr. at 150.
[79] Tagliaferri Tr. at 161-62.
[80] Gormley Tr. at21-22.

Gormley also described Boback displaying his gun in an intimidating manner:

> [] I would later discover that, I mean, **Mr. Boback, at least as far as my personal experience went, had certain bullying tendencies**….
>
> On one occasion, he entered my office and, you know, sat at a desk in front of me and reached into his sock holster and pulled out a revolver and showed me its features and functions. And I thought that that was extremely surprising, that somebody would actually have a concealed weapon in the office and then pull it out to me. And I didn't feel like he was going to use it on me, but I thought, what are you doing with this and why are you showing it to me? And I thought that was -- that was one incident. That was pretty stark.[81]

Boback never revealed to the Committee that he brought a gun to work. He was quick to suggest, however, that Hopkins carried a gun to work, out of fear of Wallace:

> [Hopkins] told me years ago, that he purchased a gun and a carry permit as protection against Mr. Wallace solely to protect -- as he felt scared for his physical existence against Mr. Wallace….[82]

Gormley also had personal knowledge of Hopkins bringing a gun to work, including one incident when Hopkins pointed a gun at Gormley:

> Q. You mentioned other Tiversa employees carried weapons in the office. Do you recall which employees did that?
>
> A. Well, one incident I remember **Sam Hopkins had gone and pulled it out and pointed at me down a hallway**.
>
> * * *
>
> Q. Did you feel threatened when Mr. Hopkins pointed the gun at you down the hallway?
>
> A. I didn't feel threatened at the time.
>
> Q. Did Mr. Hopkins say anything when he pointed the weapon?
>
> A. I don't remember him saying anything. It may have been the same day that Mr. -- they all went to the gun store, and I don't know if it occurred after or before Mr. Boback, so I may have been more sensitized to the fact that there were weapons in the office that day, silly as that sounds.[83]

---

[81] *Id*. at 18-19 (emphasis added).
[82] Boback Tr. at 205
[83] Gormley Tr. at 76 (emphasis added).

Boback also brought swords to the office, and distributed swords to Tiversa employees. According to Schultz, "Bob would hand out a sword to each new employee that he thought represented their character… I believe mine was like a Marine sword or something based on my time at Wharton and a few other things that he thought fit my character… Someone else got the sword Gandalf carried in *The Lord of the Rings* because he thought it fit their [*sic*] personality."[84]

The Committee learned of one instance where an employee attempted to take action against Boback and his intimidation tactics. Gormley described a professional disagreement he had with Boback over handling a forensic analysis issue. In a response that the Committee has found to be typical, Boback sent Gormley a threatening e-mail. Gormley testified about the incident:

> Mr. Boback and I had a dispute as to how to handle the scope of that particular exercise [regarding how narrow or broad search terms should be kept for a prospective client]. I don't think either one of us were right or wrong… I contended that we should provide the whole. He contended that we keep it more narrow.
>
> We had a very stark disagreement on how to handle that…And this was a highly negative—well, a very stark email to this effect sent to me, as well as a phone call later that evening when I was at an event with my daughters at school. And he told me to keep it within the scope he told to me, to keep it, **or else there would be consequences—in other words, either terminations or significant consequences**.
>
> [T]hat's what motivated me to go to Mr. Becker.
>
> **I was actually quite concerned to go to Mr. Becker because I feared retaliation**.[85]

From that point forward, Gormley chose not to confront Boback because he felt that it "usually wasn't very productive, because [Boback] would come at you and tuck it away as something that potentially could be used later."[86]

When Boback heard that a Tiversa employee had approached the board with concerns about his professionalism and leadership, he became irate and sought retaliation:

> I was very concerned about retaliation or being—it turned out that the feedback I gave to Mr. Becker, I believe, was incorporated through various actions the board had taken… [T]here was a point in 2008, in September, early September, where Mr. Boback called me up and said he'd just received a review and some feedback from the board, and one of the elements was that an… employee in the company had given that [negative] feedback. And he was extremely angry about that and **wanted**

[84] Schultz Tr. at 112-13.
[85] Gormley Tr. at 25-26 (emphasis added).
[86] *Id.* at 30.

> **to know who that person was, and he was going to take whatever measures it took to find that out**.
>
> In the subsequent week and a half, **he held individual meetings with each person and also held a group meeting where he asked each person in the executive team, did you say it, did you say it?** And he suspected that [redacted name], an employee of the company, may have been the person. My guess is he also suspected me. I denied that at the time, out of concern for my own wellbeing I guess. But he wouldn't let it go.
>
> * * *
>
> He came into my office, everyone had left, shut the door, sat in the same seat that, you know, the pistol and everything had been pulled out, and basically kept asking me questions in different ways to see if it was me[.]
>
> * * *
>
> Now, he also said that… **he thought it was [redacted] and that I needed to fire [redacted] because he suspected that it was her**. [Redacted] happens to be a personal friend of mine, somebody I brought into the company. So I was in a very conflicted situation, because I either fire somebody that I know didn't do it or I admit that I did it. So I told Mr. Boback that it was me that evening and told him why, you know, went through some of the major reasons that I mentioned that I gave to Mr. Becker.
>
> * * *
>
> But, after that point, **there was a lot of fallout that I believe occurred because of that incident**. And it was a very difficult period for me personally at the time, **because at that point I was ostracized from the rest of the company**, had to apologize to different people within the company for having went [*sic*] out the chain of command and saying things, that, in Mr. Boback's view, weren't true.[87]

Soon after, in September 2008, Gormley was demoted from COO to "Vice President of Data."[88] Boback explicitly told Gormley that the demotion was the "outcome [of] those discussions with the board."[89] Nonetheless, Gormley tried to perform his new job. Boback, however, refused to let Gormley succeed. Gormley testified::

> This is in 2009, and as part of the data business, I was involved on a potential acquisition of the company by Experian. Mr. Boback and I got into an argument about how to interact with Experian in that discussion. I

[87] *Id*. at 31-32 (emphasis added).
[88] *Id*. at 33.
[89] *Id*. at 33-34.

> wanted Lisa Frankovitch to be the person who would interact with Experian and then have Mr. Boback back her up in the discussions. He didn't agree.
>
> We had a disagreement about that, and **subsequently he just said, "Joel wants you off the deal**," meaning this board member wants me off the deal. This is subsequent to [the]… first board meeting, and I didn't believe that that was the case. I reached out to Lisa Frankovitch, who had that relationship, but then she suggested I talk to Joel directly. I called him up, and he indicated that **he never said that, and he said that I should go talk to Bob and make that clear**. So it was—at the time it clearly caught up with him, no, he didn't, Joel didn't actually state that. So that was one indication.[90]

Gormley was terminated in late 2009, he believesin retaliation for reporting Boback to Tiversa's Board of Directors.[91]

Boback's intimating comments did not end even after Gormley was fired:

> Q. Have you had any other communication with Mr. Boback since your termination? I don't know if threats of litigation counts, but have you had any communication with Mr. Boback following your termination?
>
> A. Yes. The points of communication after termination, I guess the first time he communicated with me, I decided not to sell some options that I owned in approximately 2011, and he sent me an email that started with "LOL, LOL, LOL." That means -- you guys know what that means -- "laugh out loud, laugh out loud." And **he ridiculed me for not selling my options and then made fun of my role as the director of downstream marketing and just sent that to me out of the blue**. And I still have that email. That was 2011.[92]

The Committee has further learned that Boback is continuing his intimidation tactics toward former employees that have cooperated with this Committee's investigation. Tiversa has refused to pay legal fees that Gormely accrued while cooperating with this investigation and the FTC matter against LabMD, despite an agreement with Tiversa that he would be indemnified.[93] Boback has further sued Richard Wallace and lawyers representing LabMD in a defamation action in Pennsylvania. Such witness intimidation tactics are unacceptable.

---

[90] *Id.* at 89-90 (emphasis added).
[91] *Id.* at 87-88.
[92] Gormley Tr. at 147 (emphasis added).
[93] E-mail from Dwight Bostwick, Att'y for Christopher Gormley, to H. Comm. on Oversight & Gov't Reform Majority Staff (Nov. 20, 2014, 4:40 p.m.).

E. Boback has not been forthcoming regarding the nature of his close relationship with Wallace, or the central role Wallace played at Tiversa

In advancing the narrative that Wallace is the source of all of Tiversa's problems, Boback has repeatedly contradicted his own statements to the Committee. Often, instead of answering the question asked, he instead spoke tangentially about Wallace's bad character and dangerous propensities.

Tiversa recruited Wallace in mid-2007.[94] Wallace was given substantial responsibilities at Tiversa. In his professional duties, Wallace was tasked with "reflect[ing] the technology of Tiversa to customers when they would come in."[95] Wallace was "many times called out to be the expert technical person in the data store area of our office."[96] Wallace also was Tiversa's face for the FBI, and spent around 20-30% of his time "doing work related to the FBI arrangement."[97] A former Tiversa employee said that Boback "absolutely" trusted Wallace's work.[98]

Boback would like the Committee to believe that Wallace was and continues to be the source of all of Tiversa's problems. If that were true, Boback would be in gross dereliction of his official duties as CEO of Tiversa. However, accounts of multiple Tiversa employees indicate that Boback and Wallace shared an exceedingly close relationship, and that Boback leveraged his status as CEO to manipulate Wallace to act on his behalf.

Numerous Tiversa employees have characterized Boback and Wallace as close, and testified that the two spent a great deal of time together. As one employee stated :

> **[T]hey were together constantly**… Mr. Wallace tended to know where Mr. Boback was. If you needed to know where Mr. Boback was, you'd ask Rick, or Molly Trunzo would ask Rick, because many times he knew where Bob was.
>
> * * *
>
> **I mean, my perception of Mr. Wallace was that he was Mr. Boback's spy.** And I think one on one I had a decedent relationship with Mr. Wallace, but I think when he was in a group or he was with Mr. Boback, he became different, and he tried to show his worth, I think, in multiple ways with Mr. Boback.[99]

Troublingly, numerous Tiversa employees described Boback and Wallace following cars together. Czarnecki stated that he heard "some kind of talk about [Boback or Wallace using a

---

[94] Gormley Tr. at 176-77.
[95] *Id*. at 50.
[96] *Id*. at 50.
[97] *Id*. at 86.
[98] *Id*. at 178.
[99] *Id*. at 48-49 (emphasis added).

GPS device] at the old offices"[100] to track a specific individual.[101] Another former employee also heard Boback and Wallace talk about putting a tracking device on a vehicle.[102] Gormley believed that he would be followed after he approached a board member with concerns about Boback's professionalism, "because there was a history of Mr. Boback and Mr. Wallace following people for fun, you know. And so, in this instance, I felt like they may follow me and, you know, a retaliation may occur[.]"[103]

Ultimately, statements made by Boback impugning Richard Wallace simply do not add up with the facts of Wallace's employment while he was at Tiversa.

a. Wallace received only a glowing performance review while a Tiversa employee.

Wallace received one review during his tenure at Tiversa. This review, given in 2008, described Wallace as a talented analyst and consummate professional. Among his "key accomplishments," the review stated that Wallace:

> Led the work and served as an official informant to F.B.I. related to child pornography on P2P file sharing networks. Rick also managed the day-to-day relationships with two F.B.I agents. This work was new to Tiversa and Rick handled the many ambiguities associated with this work in a highly professional manner that was respected by his F.B.I. counterparts.[104]

The review describes Wallace as "critical in aligning Tiversa for a potential deal with the Air Force Office of Special Investigation," and "*instrumental* in a number of press events serving as an expert for reporter research."[105] The review stated that as a cyber forensic analyst, Wallace "monitor[ed] accounts of Cigna, American Express, and PGP and [was] a core Cyber Forensic Analyst with, for example, University of Florida, Wagner, Wachovia, GE." Wallace also "contributed insight into the design and operation of Tiversa F.A.S.T. productivity suite which whwen fully implemented should substantially improve CFA productivity."

The review listed Wallace's strengths as the following:

> <u>Work Ethic</u>
> Rick has an outstanding work ethic and can always be relied upon to put in the extra effort surrounding a project or finding files to support a Tiversa business opportunity. There have been many weekends and/or late nights where Rick has worked extra hours either in the office or at home to make Tiversa's business objectives happen.

[100] H. Committee on Oversight & Gov't Reform, Transcribed Interview of Orion Czarnecki, at 72 (Sept. 16, 2014) [hereinafter Czarnecki Tr.].
[101] *Id.* at 72.
[102] *Id.* at 40-41.
[103] Gormley Tr. at 26.
[104] Tiversa, 2008 Review of Richard Wallace (Aug. 4, 2008).
[105] *Id.* at 1 (emphasis in original).

> Client and Media Relations
> Rick has received exemplary feedback for his work from client contacts most notably from F.B.I. and Cigna. Rick has also managed relationships and provided P2P background to outside parties and media during their investigations of P2P risks.
>
> Drive for new business / press
> Rick is constantly scanning the P2P (literally) for files or individuals that will yield new Tiversa business, yield more tickets for existing Tiversa clients thus strengthening Tiversa's value with existing clients, and finding situations that put the P2P or Tiversa in a strong public relations position. Rick always seems to be able to find a hard hitting file or P2P situation to accelerate our client acquisition, existing relationships or to help serve as a nugget for a powerful news story. For example, recently Rick found a number of American Express internal files in the Philippians [*sic*] which have strengthened our relationship with Amex's CIO and put us in contact with Accenture.
>
> Enthusiasm for the P2P Space
> There is no other person at Tiversa that lives and breathes P2P more than Rick. His level of enthusiasm for finding P2p sourced information is contagious and extremely valuable to Tiversa.[106]

Going forward, the review pointed to two areas in which Wallace could improve. First, the review suggested that Wallace "[c]onsider [d]ownstream [a]ffects [*sic*]" by

> [N]ot only continu[ing] his outstanding work as an individual contributor, but [] seek[ing] to make the whole team more effective, more highly scalable, less Dilbert-like by balancing the short term needs for sales and files with the long term need to make everyone effective and ready to handle more scale. I would ask Rick to please provide me direct feedback on areas that he thinks can be more effective and to **take a leadership role** in addressing the issue.[107]

Second, the review suggested that Wallace pursue searching other peer-to-peer networks for "'veins' of file gold":[108]

> **Rick is a maestro of LimeWire operation and sleuthing. The business benefits greatly every time we find more "veins" of file gold not only including sources on LimeWire, but on wholly new P2P networks.** For instance, the addition of eDonkey to our roadmap was guided by the large magnitude of sensitive files that appeared by using the eMule client in

[106] *Id.* at 1-2.
[107] *Id.* at 2.
[108] *Id.*

> Tiversa's lab. In between leveraging LimeWire for the benefits already highlighted above, I would like Rick to experiment with other clients to discover new caches of files and help guide our product roadmap.[109]

In consideration of his performance, the review noted that Wallace was to be given a 9.8% raise, in addition to the 20.6% Wallace received at the end of 2007. [110] The review concluded by congratulating Wallace on his achievements.[111]

It is not clear who at Tiversa wrote Wallace's review. Gormley stated that he, Schultz, and Boback would have all had input on the review.[112] Although Schultz was Wallace's direct supervisor, and although Schultz reported to Gormley, Boback gave Wallace a direct raise without telling either of Wallace's supervisors.[113] This caused Gormley to think that he, Schultz, and Boback "had split responsibilities for Mr. Wallace."[114]

Tiversa employees characterized their relationships with Wallace as typical professional relationship. Tagliaferri stated that he and other Tiversa employees socialized with Wallace:

> Q. Did you socialize outside of the office with Mr. Wallace?
>
> A. Sometimes. If he would have a bonfire or a Christmas party or something like that at his house then I would attend something like that.
>
> Q. And were these events attended by Tiversa employees generally?
>
> A. Sometimes. There might be, you know, a couple of other Tiversa employees there, and other professionals in the security industry that we all work with that may attend one of his get togethers.[115]

When asked to describe Wallace's professional contribution to Tiversa, Tagliaferri stated:

> [Wallace] found a lot of information that was very sensitive, confidential and bad stuff out on these networks that shouldn't be out there, and he was really good at finding information out on the networks.
>
> And, to that extent, you know, would we have found that information without Rick? I don't know. Maybe we would have**. But the things that Rick found certainly contributed to the company. He was an asset to the company to that extent**.[116]

---

[109] *Id.*at 2-3.
[110] *Id.* at 3.
[111] *Id.*
[112] Gormley Tr. at 205.
[113] Gormley Tr. at 55.
[114] Gormley Tr. at 55.
[115] Tagliaferri Tr. at 156.
[116] Tagliaferri Tr. at 98 (emphasis added).

Boback and Wallace's relationship extended beyond the professional. When Boback and Wallace interacted in the office, it was not through the traditional hierarchical channels:

Q. Mr. Boback was the CEO, correct?

A. Yes.

Q. And Mr. Wallace was an analyst, correct?

A. Mr. Wallace was an information forensic engineer.

Q. And so, in the corporate hierarchy, Mr. Boback was certainly above Mr. Wallace, correct?

A. Yes, substantially.

Q. Is the type of direction that Mr. Wallace took from Mr. Boback typical to the type of direction that other employees in Tiversa took from Mr. Boback? Or was there something different about the nature of the direction that Mr. Wallace was taking from Mr. Boback?

A. It was much more one-on-one, less hierarchy involved. It wasn't like Mr. Boback went to me and then I went to Mr. Schultz and then Mr. Schultz went to Mr. Wallace to ask him to do something. **It was, "Hey, Rick, you're coming with me," and off he went. Or, "We don't know where Rick is. He's with Bob."** It was much more direct. **So it was independent of any kind of hierarchy that existed**.[117]

Another Tiversa employee verified that even though Wallace was a forensic security analyst, he reported directly to Boback.[118] According to a former Tiversa employee, Boback and Wallace were very close, with Boback exerting greater influence over the relationship:

Q. Would you describe them as close friends?

A. Yeah, absolutely… **[T]here was nobody that was closer to Bob in the time frame that Rick was there than him**, with maybe the small exception of Mr. Hopkins, but even Mr. Hopkins had his own life, and he just wanted to go do his thing. Mr. Wallace and Mr. Boback were tied at the hip.

[117] Gormley Tr. at 214-15 (emphasis added).
[118] Tagliaferri Tr. at 75 ("[M]y understanding was that he reported to Mr. Boback.")

Q. You would say they're close friends?

A. Yeah, I would say that.

Q. **Would you describe one of them as having a dominant role in the friendship?**

A. **Yeah, Mr. Boback.**

Q. Could I ask why you would say that?

A. Well, Mr. Boback had a bigger house, he had all the little—you know, the toys and games, and so that would certainly lead the way, and just the way they interacted with one another. **It was clear that Mr. Wallace was taking direction from Mr. Boback, not the other way around**.[119]

Boback, on the other hand, has consistently mischaracterized Wallace and his responsibilities to the Committee. When asked a simple question about what duties Wallace performed at Tiversa, Boback could not give a straight answer:

Q. Okay. When Mr. Wallace was employed at Tiversa, which section or sections did he work in?

A. I don't know that he necessary -- he really didn't work in -- he was never a cleared individual, so he never had the clearance portion of it when everyone else went through there**. Mr. Wallace's role at Tiversa was regarding, or most of his work was child pornography**, searching for child pornography and providing it as a confidential informant to the FBI, and also identifying new cyber risks for, you know, educational purposes that he would then provide to me and then whenever I would go, I've traveled around the country training law enforcement for FBI LEEDA, L-E-E-D-A and he would sometimes travel with me and, you know, highlight different risks for the cyber world that law enforcement wouldn't see otherwise.[120]

* * *

Q. Was Mr. Wallace first hired as an analyst?

A. Yes, he was.

[119] Gormley Tr. at 180 (emphasis added).
[120] Boback 62-63 (emphasis added).

Q. And when was he first hired by Tiversa as an analyst?

A. I'm not sure exactly, but I think in 2007, maybe. I'm not sure of the exact date, but the summer roughly, I think I remember around the summer of 2007.

Q. Was Mr. Wallace first hired for his skills as an analyst or for his work with the FBI?

A. No, Mr. Wallace was hired as an analyst. Mr. Wallace was a stay-at-home dad in Illinois and his wife was in the military, and Mr. Wallace ran a Web site called SeeWhatYouShare.Com. Essentially, See What You Share, what he did was, he would search for files leaked or exposed on file-sharing networks and he would publish them on his Web site. Essentially, he was the first iteration of WikiLeaks, but he did it under the SeeWhatYouShare.com website.

So an individual, Tom Sydnor, Thomas Sydnor who used to work at -- work with Senator Hatch in the Senate Judiciary, Tom Sydnor told me about this Richard Wallace and said, hey, you should talk to this guy because he's, you know, in the space that you're in where no one knows anything, he's doing some searches that may be of interest to you, and he said, he's a little different but you should talk to him.

So we flew him to Pittsburgh, we met with him and then we offered him as a job as an analyst and that's how he started, as an analyst in our corporate business and that's what he started with a reporting structure of he reported to an individual by the name of Griffin Schultz who reported to the chief operating officer, Chris Gormley, who then reported to me.[121]

* * *

Q. At what point did Mr. Wallace's work transition from part time for the FBI and full time for the FBI?

A. **Mr. Wallace was very erratic in his time, so I'm not sure. Sometimes you'd see him; sometimes you wouldn't, in the office.** And he was -- I'm not sure. **It was mostly FBI work. Again, he didn't generate revenue so therefore it was hard for me to say**, I couldn't tie it to revenue coming in so I didn't know, you know, what he was doing.

[121] Boback Tr. at 64-65 (emphasis added).

> So he, you know, that's how that went. So, I mean, he was still working as an analyst, obviously, in 2008 and then he, like I said, he was doing both work and then it kind of transitioned out, probably closer to 2009, 2010.[122]

Expanding on the assertion that Wallace did not generate revenue, Boback told the Committee that Wallace and personally received cash payments from the FBI as a confidential informant, while Tiversa did not receive any money as a result of Wallace's FBI affiliation:

> Q. So Mr. Wallace worked with the FBI. It sounds like he was, at times, working in the business-to-government section. Is that fair?
>
> A. But we didn't have any contract with the FBI, so that's why I don't necessarily know where to put him. **He was not a revenue generating** [*sic*]. In fact, recently it's come to light that Mr. Wallace, it's our understanding that **Mr. Wallace was receiving revenue from the FBI as a confidential informant, yet none of that money ever made it to Tiversa**. So he was keeping that money, that cash that was being given to him, at a reported, as we were told a reported $1,000 per child pornography case that he gave to the FBI.[123]

However, a former Tiversa employee told the Committee that Tiversa—or at least Boback—was compensated in cash for Mr. Wallace's work with the FBI:

> Q. And do you know whether Tiversa received any compensation from the FBI for Mr. Wallace's work?
>
> A. Yeah. **They were paid cash. I don't know how much. I recall one instance where there was a bag of cash on Molly Trunzo's desk, and it was apparently from the FBI.**
>
> Q. As someone who was responsible, in part, for –
>
> A. About this much. [Estimating the size of the bag].
>
> Q. -- overseeing financial controls at Tiversa, were you concerned that the FBI was paying the company in bags of cash?
>
> A. Yeah.
>
> Q. Did you raise those concerns with anyone at the company?

[122] *Id*. at 75 (emphasis added).
[123] *Id*. at 63 (emphasis added).

A. This was after my review of Mr. Becker. Yeah, I -- well, I'm trying to remember if I raised those concerns. I definitely raised the concerns during the arbitration hearing, you know, because I wasn't sure whether that was being recorded properly.

The relationship with the FBI itself and how it was set up, I remember Griffin Schultz making a comment and me making a comment at the time as to how we thought it should be handled. And that was another instance of Mr. Boback lashing out at Mr. Schultz. I remember that.

And that was on my -- actually, it was on my comments to Mr. Becker. I remember telling Mr. Becker about any cash and the FBI because I don't know that they were paying us at that time. I think it was just an initial, kind of, trial.[124]

Gormley, the CFO, was apparently not made aware of the cash payments prior to seeing them on Trunzo's desk, and could not say if the money was properly placed in an account.

Later in his transcribed interview, Boback contradicted himself in admitting that Tiversa had received a cash payment from the FBI, although he insisted the money went to Wallace:

Q. But you don't have any specific information about anything that he downloaded?

A. He's a confidential informant, and we didn't know. But as I mentioned before, early on Mr. Frankhouser talked to me about knowing that Rick Wallace was on Tiversa's payroll and downloading child pornography presumably for their prosecutions. He discussed paying Tiversa as a confidential informant, of which I think he did. I mean, he may have -- they may have paid us as a confidential informant a little bit. I could double check. I'm not positive. **They may have paid us some money as a confidential informant**.

Q. So as you understand it, Tiversa is a confidential informant as opposed to Mr. Wallace, personally?

A. I don't know how the FBI designates it, you would have to look. I know that it ultimately became Mr. Wallace. He said to me, he being Mr. Wallace, said to me, along the way that for work he has been doing with the FBI, he was owed some money, and he was owed so much as a confidential informant. It was like $1,000, or $2,000, or something like that.

[124] Gormley Tr. at 209-210 (emphasis added).

> **And he said to me, would I mind if he took that as a bonus because he has been doing so much hard work for this. I said, no, I don't mind, meaning put the cash into the account at Tiversa as we always do, record it, because we wanted our revenue to come up, and then we will add the amount to your check with the proper withholdings**, and that was the last time, thinking back, that was the last time I ever heard anything talked about money paid as any informant and it's my allegation that he continued to take that money, at a rate of roughly $1,000 per case, in cash and he took it. So I reported that to the authorities.

Q. I see. And the FBI was paying Tiversa for the information that Mr. Wallace was providing, is that right; there was some kind of contract?

A. No.

[Att'y] No, he didn't say that.

Q. Nothing?

A. Nothing.

Q. I'm sorry if I misunderstood.

A. Yeah, no. It is my allegation that **Mr. Wallace was paid by the FBI as a confidential informant, from monies that should have been directed through Tiversa because he was doing that under our direction and we were paying him a salary to do that**, as I mentioned to you and he decided to take that money himself, which is larceny. [125]

In a separate instance, Boback described Wallace's professional behavior as "normal" before launching into a tangent about how Wallace had a "revenge-based mentality":

Q. How often during the course of his employment at Tiversa, if you could describe it for us, was Mr. Wallace in the office? Was it daily?

A. Yeah. I mean, **he was in there like a normal employee, for the most part. I mean, he would come in and leave just normal**.

Q. Earlier today you mentioned he worked from home a lot and you didn't really know what he was doing.

[125] Boback Tr. at 120-122 (emphasis added).

A. Well, he worked -- as I testified to, he told us that the best time to catch child pornographers was in the evening. So his working from home was over the night, like at nighttime.

Q. Okay. So –

[Discussion off the record.]

[Att'y] If you could just be clear on that.

A. So he would be in the office and then he would go home and search. I think that Mr. Wallace searched peer-to-peer quite a bit as a part of his normal -- it was almost like his ritual, if you will, for his life, to where he was always searching.

Like he was always in front of a computer screen and always searching something, either online or searching peer-to-peer, whether it was at the office or whether it was at home. He was always –

Q. Did you find that troubling?

A. I work in tech. Everyone's a little bit different. So, I mean, we have -- in tech, you know, you have different personalities. He was no exception of a different personality.

The downside of one of the things that **you recognize is he had a very revenge-based mentality[.]**[126]

However, Boback described Wallace's duties as much more expansive when the discussion turned to verifying the truth of his testimony before Congress. Boback testified that Wallace was solely responsible for Boback's testimony before this Committee in 2009. Thus, according to Boback, any blame for inaccuracies in the testimony should fall on Wallace. Boback testified:

Q. Did Tiversa employees identify the source of this information other than France? In other words, France got it from somewhere, so do you know where France got it from? Did Tiversa employees determine that?

A. **You're asking me to testify to what someone else did? I have no idea. I was provided information that I testified to, which I believed to be rue and correct, as I just testified to again.**

[126] *Id. at* 202-03 (emphasis added).

Q. Yeah, no, no, I hear you. I'm just asking you if you know anything else about the facts underlying.

A. **I know that Mr. Wallace would have been doing this type of work and provided this information to me, which I then provided, believing it to be true and correct, to Congress.**

Q. Can you tell us with a little bit more specificity what the information Mr. Wallace provided to you was?

A. Sure. Again, this was 5 years ago, but **Mr. Wallace would have been responsible for discussing breached files; finding, downloading breached files; locating the location of where those files came from; and then, you know, articulating that to us**. So, you know, producing that information, so therefore any information that I received regarding where a file came from, who was the disclosing source, the file itself all came from him.

Q. And did he tell you those things?

A. Yes.

Q. The source?

A. Yes.

Q. The location, the specific location?

A. Yes.[127]

* * *

Q. Just to clarify for us, my understanding -- and please correct me if I'm wrong, but my understanding from our earlier conversation was that, you know, **Mr. Wallace was hired, you used the term charity with respect to him working at Tiversa**. I understood that **Mr. Wallace was working primarily on child exploitation or child pornography cases, did a lot of that work from home, and I believe you said you didn't really have a great idea of what he was doing a lot of the time**. So the work that you testified to seems to fall outside the bounds of how you described Mr. Wallace's responsibilities at the company earlier. **Could you help rectify that for us?**

[127] *Id.* at 107-09 (emphasis added).

A. **I don't think it needs rectification**, but this -- maybe you misunderstood what we were saying. Mr. Wallace did do child pornography-type work with the FBI, to the best of my knowledge. **Mr. Wallace, as I already testified to, was an analyst at Tiversa, which then would put him in this information**. He also searched for, on his own, in the time when he was searching his child pornography and other things, he would come up with files. **He would download files outside of our system**, because, as I testified, our system was configured to look for a dynamic signature profile which was specific for each client, which does not just take everything. So therefore, Mr. Wallace would come up with random downloads that, again, because he managed to do the search from end to end, we were confined within a very confined space in the confines of our work product.

Mr. Wallace could put whatever search in at any time. Clearly, as I testified to, I wouldn't have searched for U.S. nuclear information. However, Mr. Wallace apparently came up with this U.S. nuclear information, because, again, he could put whatever search in and see the outcome of it. So therefore, when he came to me and said, here, I have this, this is not through the course of our normal work of Fortune 500 clients. So therefore, he was putting whatever search in any time he wanted to then -- I'm assuming, because then he would come up and provide us these files, and then he also detailed where the file was -- where he downloaded it from**. I had no reason to believe it wasn't true, and I testified to that accordingly**.[128]

Boback reverted again to describe Wallace's role as minimal later in the interview. He stated:

Q. Have you hired anyone to replace Mr. Wallace's work as an analyst for Tiversa?

A. No, he hasn't been an analyst for years, so he hasn't logged in for a long time.

Q. I'm just -- I'm confused about this aspect of it, though. I can't get my head around it --

A. Yeah, okay.

Q. -- because is he doing work just for the FBI, or is he acting as an analyst? What -- I just -- sorry, I keep asking the same question. I want to understand, though.

[128] *Id. at* 110-11 (emphasis added).

A. Yeah, that's okay. He was not -- in my estimation he was not -- **now, granted nobody watched him**. Like on a daily basis, nobody would say, what is every minute of your day happening? So that was out. **But he was not an analyst. He was not sitting in what the analysts do for years**.

* * *

There was never like one job, specifically that, that's all it was. He could be researching how to delete metadata or do something along those lines. He could be researching other cyber crimes. So he was kind of doing this mix hodgepodge of a bunch of different things.

Q. But he wasn't doing work for Tiversa's other clients?

A. Correct.[129]

As noted above, multiple current and former employees described Boback and Wallace as exceedingly close, both at and outside of work. To the Committee, however, Boback repeatedly characterized Wallace as a dangerous alcoholic. Boback told the Committee that he was aware of Wallace's poor performance and inappropriate behaviors but failed to terminate him for years, even though Tiversa had terminated numerous other employees during the same time period.

When staff questioned Boback's judgment in continuing to employ Wallace in the face of his purported poor performance and erratic behavior, Boback evaded questions with convoluted tangents about how unwell Wallace seemed or the dangers he allegedly posed. He failed to address his own decision-making, instead highlighting at length Wallace's destructive personality.

F. Tiversa's Unseemly Business Practices

1. Tiversa used fearmongering tactics to generate business

From its inception, Tiversa has marketed itself as a vital tool to be wielded against the "scary" and complex world of the peer-to-peer network. Tiversa largely creates revenue through contracts with companies who desire cybersecurity services. To build their brand and generate clientele, Tiversa uses fearmongering tactics by citing stories of the very most sensitive documents on the peer-to-peer falling into the hands of criminals and terrorists.

Sam Hopkins, the creator of Tiversa's technology, gave the Committee examples of the type of information Tiversa had found on the peer-to-peer network. He stated, "I didn't want to

[129] *Id.* at 251-52.

see the stuff, so I just stayed out of it all….There's just scary stuff out there."[130] When asked to explain, Hopkins continued, "Yeah, I mean everyone knows of Snowden. Tiversa has way more than he does and Tiversa has new information on everybody."[131]

Hopkins further described files he had seen during the course of his work with Tiversa:

Q. Let's fast-forward to the discussion of the Marine One schematics. You said at one point that the Marine One schematics were, sort of, the least sensitive thing you've seen. Is that fair?

A. I wouldn't say "least." You know --

Q. One of the least.

A. -- a tax return for somebody is probably the least, but definitely not the scariest. **Scariest would be how to fly a 747 sitting in, you know, the hands of an Arab. You know, that was pretty scary.**

Q. And you've seen that on --

A. Oh, yeah.

Q. -- the peer-to-peer networks?

A. Yeah. **Or, you know, some guy collecting tons of explosive information from the military and also how to tow a boat into the harbor in the Pacific, you know**. Or one of our -- or **all of our bases in the South Pacific, all of their security cameras, exactly where all the gunners are and what the cameras can see and how to gain access, that's pretty scary.**

How to blow up every, you know, big city in America with improvised explosives and exactly what trash cans to stick them in and how to take out bridges, that's pretty scary. Space-based laser stuff, that's pretty scary. Seeing China, Russia, Iran actually grabbing the stuff and seeing it transferred over to them, that was pretty scary.

Q. So who created these documents?

A. Government agencies. Defense contractors.

Q. And these are all in the Tiversa data store?

A. They're out on the peer-to-peer, and Tiversa has some of them.

[130] Hopkins Tr. at 26 (emphasis added).
[131] Hopkins Tr. at 26 (emphasis added).

Q. But everything you just described, is that in the possession of Tiversa in its data store?

A. **That's where I've seen them, yeah. And, I mean, there's millions of files. I mean, it's everything -- I would not be shocked if everybody's information in this room is sitting out there, from your doctors and accountants and, you know, whatnot. It's out there.**

[Att'y] To be clear, when you say in possession of Tiversa, it's not exclusively in the possession of Tiversa. You got it off the Internet.

A. Yeah, it's peer-to-peer. It's probably still out there, and anyone could go and grab it.

Q. But at the time you viewed this information, it had been downloaded by Tiversa.

A. Yeah.

Q. Were these documents marked "classified," do you know?

A. **Oh, yeah. Tiversa is, and peer-to-peer in general, there's tons and tons of classified.** And Tiversa turned over -- Tiversa was in the strange situation, not so much anymore, of that, you know**, they had droves and droves of classified information on all the wars that were going on over in the Middle East. We could see what was happening every day, with all the stuff that was being leaked**. And the government would come every once in a while and get it, and then, you know, it would just sort of disappear, you know[.][132]

Hopkins statements about Tiversa routinely downloading classified information is at odds with what the Committee heard from Tim Hall. Hall told the Committee that much of the information Tiversa provided to him while at NCIS was unclassified.[133] Hall also stated that, since he began working for Tiversa, Tiversa had not determined that it was in the possession of a classified document.[134]

Regardless of how often Tiversa actually downloaded classified information, however, their marketing tactics appear to have worked—Tiversa frequently received press regarding its account of the government security leaks. When Hopkins was interviewed by CNET regarding Tiversa's involvement in the Marine One leak, he stressed the wide-ranging nature of inadvertent leaks on the peer-to-peer, even designating it as "the biggest security problem of all time":

[132] Hopkins Tr. at 97-99 (emphasis added).
[133] Hall Tr. at 39-40.
[134] Hall Tr. at 35.

Q. So your team concluded that the materials fell into the hands of Iran. Is it possible that other actors also are trying to take advantage of similar openings in the system?

A. Heck yeah. Every nation does that. **We see information flying out there to Iran, China, Syria, Qatar--you name it. There's so much out there that sometimes we can't keep up with it.**

Q. I would have assumed military contractors would use more secure networks to communicate.

A. Everybody uses (P2P). Everybody. We see classified information leaking all the time. **When the Iraq war got started, we knew what U.S. troops were doing because G.I.'s who wanted to listen to music would install software on secure computers and it got compromised.**

Q. This is what your company specializes in, obviously, but what's your professional opinion about the extent of this sort of thing?

A. **This is the biggest security problem of all time**. Coming from me, it sounds biased. But you can get 40,000 Social Security numbers out there at the drop of a hat. **We've had people come into our data center and we've shown them things that are out there on P2P and they go away with their minds blown**.[135]

Various outlets portrayed Tiversa as partnering with federal authorities. One outlet wrote, "By the end of [2004], Tiversa was working with the CIA, FBI, Homeland Security, and the U.S. Secret Service."[136] Regarding a WikiLeaks spreadsheet containing potential terrorist targets in California, another outlet wrote, "Asked to aid in the investigation of the leak by U.S. authorities that the company declined to identify, Tiversa found the spreadsheet was inadvertently exposed by a California state employee using a peer-to-peer network in August 2008, more than a year before WikiLeaks posted it."[137]

Tiversa capitalized on this press in their presentations at various conferences and to potential clients.

2. Tiversa systematically mined for files for "potential" clients as a solicitation tactic.

[135] Charles Cooper, *Q&A: Tiversa Co-founder Talks About P2P Leak*, CNet (Mar. 1, 2009), *available at* http://www.cnet.com/news/q-a-tiversa-co-founder-talks-about-p2p-leak/ (emphasis added).
[136] John Foley, *Your Data And The P2P Peril*, InformationWeek (Mar. 13, 2008), *available at* http://www.informationweek.com/your-data-and-the-p2p-peril/d/d-id/1065643?page_number=2. The Committee found many of Tiversa's claims regarding its relationships with federal agencies to be greatly overstated.
[137] Michael Rile, *WikiLeaks May Have Exploited Music Networks to Get Data*, Bloomberg (Jan. 20, 2011), *available at* http://www.bloomberg.com/news/2011-01-20/wikileaks-may-have-exploited-music-photo-networks-to-get-classified-data.html.

A whistleblower told the Committee that Tiversa kept dossiers of information on various companies and executives in an attempt to garner new business. According to the whistleblower, Boback even went so far as to create false documents containing large amounts of sensitive information he obtained through his improper use of a law enforcement database to trick potential clients into purchasing Tiversa's services.

As a matter of practice, Tiversa contacted companies whose documents it found on the peer-to-peer network. Tiversa did so under what it called a "duty of care" policy. However, Tiversa held back critical information from companies whose documents were actually exposed in order to force them to purchase Tiversa's services.

When asked whether Tiversa contacted non-client companies about documents actually exposed on the peer-to-peer network, Boback told the Committee that it did not—that Tiversa only searched the data store for potential clients that had a relationship with Tiversa. He then admitted that Tiversa did in fact "cold call" new clients with documents found on the peer-to-peer network, but stated that it was not a "routine practice." He testified:

Q. Can you describe circumstances in which you would mine the data store for a potential client?

A. If the client -- if we know we are **-- if we were contacted or we have some relationship with a certain client and we know we are going to see that client**. Prospective clients, yes, prospective clients and the prospectives, it usually starts with a phone call with a prospective client, as any prospective client would start, you have a phone call with the client. You explain to them about the risks of file sharing, the risks of, you know, what this is, and how information can get out this way.

Most people don't understand it, and they say, can you give me an example, so we go into the data store, not into Eagle Vision. We go into the data store and we usually prepare an example sheet of whatever we have in the data store without looking for it; providing that example –

Q. **Have you ever contacted a potential client after mining the data store for information concerning that potential client?**

A. **I think I -- you lost me there.**

Q. Absolutely. **Have you ever looked in the data store for information, found information, and then contacted a potential client?**

[Att'y] **He can't answer. I'm not sure I'm following you. So company X, we want to get them. Let's look for stuff on company X. We call company X?**

Q. Correct.

[Att'y] Okay, do you follow that?

A. Yes. **No, I don't believe so. We may have, but I don't believe so. It is not a routine practice by any means**.[138]

The Committee found, however, that Tiversa routinely "cold called" clients with documents found on the peer-to-peer network. Under the company's "duty of care" policy, Tagliaferri regularly called businesses to alert them to exposed documents. In fact, Tagliaferri called companies nearly every day at some points of his employment with Tiversa.[139] The Committee also spoke with numerous companies that Tiversa contacted seemingly out of the blue about documents it found on the peer-to-peer network. Documents obtained by the Committee further reveal that Tiversa contacted MetLife, NetXert, Open Door, and LabMD regarding use of their services.

[138] Boback Tr. at 146-47 (emphasis added).
[139] *Id.* at 132.

From: ifriedman@metlife.com [ifriedman@metlife.com]
Sent: Sunday, July 27, 2008 4:56:27 PM
To: hvaletk@metlife.com
BCC: hvaletk@metlife.com
Subject: Re: IMPORTANT: MetLife Disability Census Found on Web
Attachments: graycol.gif; ecblank.gif; doclink.gif; C2030192.gif; C1078101.gif

Harry - nice work. I thought that might be the case.

Harry Valetk

"It seems Traversa [*sic*] solicits business by scanning files online, and bringing them to the company's attention."

----- Original Message -----

From: Harry Valetk
Sent: 07/25/2008 05:01 PM EDT
To: Joseph Carroll
Cc: Ira Friedman; Justin Hixson/Leg/MetLife/US@Me
Gibbons; Tom Meenan; Meghan Canty
Subject: Re: IMPORTANT: MetLife Disability Census

Hello All,

I found a July 10th article with Traversa cited in it from a separate, but similar incident involving file-sharing networks. It seems Traversa solicits business by scanning files online, and bringing them to the company's attention.

Just a thought.

==========

A Supreme Court justice's birthday and Social Security number were exposed on the Internet after a McLean, Va., investment firm employee used an online file-sharing network at his office.

Supreme Court Justice Stephen Breyer's birthday and Social Security number, and records for about 2,000 other clients of Wagner Resource Group, were stored in the company's private files. The data breach began late last year and ended shortly after a reader of a blog on washingtonpost.com discovered the information in June on LimeWire.

Wagner hired Tiversa to repair the breach.

Tiversa's chief executive said these breaches are common since many employees and contractors install file-sharing software on office computers. LimeWire, like other file-sharing networks, allow computer users to share files directly by linking computers. But Robert Boback said users don't realize such networks may make all files available, not just music or movie files users hope to share.

"This case is unique because of the high profile of the targets. The individuals on this list are at a very high risk, almost imminent, of identity theft," Boback said.

More than a dozen LimeWire members, including some in Sri Lanka and Colombia, downloaded the personal records from Wagner, according to Tiversa officials. The company was alerted after the blog reader told Security Fix blog employees about the breach and the blog contacted Wagner.

Harry A. Valetk
Corporate Privacy Director
MetLife Privacy Office
212.578.2116 (direct)
Privacy -- Pursue it. Promote it. Protect it. Preserve it.

Joseph Carroll/Pen/MetLife/US

Joseph Carroll/Pen/MetLife/US

07/24/2008 03:09 PM

To:Ira Friedman/Leg/MetLife/US@MetLife
cc:Harry Valetk/Leg/MetLife/US@MetLife, Justin Hixson/Leg/MetLife/US@MetLife, Larry Wolff/Leg/MetLife/US@MetLife, Michael Fradkin/Ins/MetLife/US@MetLife, Michael Tietz/Ins/MetLife/US@MetLife, Susan

----- Forwarded by Michael Fradkin/Ins/MetLife US on 08/02/2008 10:02 PM -----

"Ashish Joshi" <A.Joshi@Lorandoslaw.com>
08/02/2008 09:58 PM

To "Michael Fradkin" <mfradkin@metlife.com>
cc "Justin Hixson" <jhixson@metlife.com>, "Larry Wolff" <lwolff@metlife.com>
Subject important - Urgent

Michael:

Thank you for your email. I can talk with you and other MetLife pers
a.m. and 11:00 a.m. EST on Monday, August 4, 2008. Monday afternoon d
for me.

As discussed in our teleconference, a few days ago Netxert received a phone call from an agent of Tiversa, Inc. Tiversa's agent informed Netxert that confidential information containing Netxert's employees' personal information (including but not limited to the employees' social security numbers) has been breached and that this information is available on a "P2P server" on the internet. Tiversa's agent refused to disclose the identity or location of this P2P server that contained the personal information of Netxert's employees. However, Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at $495/hour. Netxert informed Tiversa that Netxert needed to see a sample of personal information that was allegedly available on the P2P server and then would take the necessary steps. Tiversa emailed Netxert a MS-Excel file that contains personal & confidential information of Netxert's employees including their first and last names, social security numbers, date of birth, ge ary details, addresses, etc.

After a preliminary investigation, Netxert has that there has been no security breach from Netxert's computer systems and/or se tronic file that wa

to Netxert by Tiversa contains metadata that shows MetLife as "author" of the Excel spreadsheet states "MetLife Census for Disability" as its heading. The inform contained in the spreadsheet was sent to MetLife by Netxert's staff at some point in in order to obtain disability insurance. At this stage, it appears that MetLife is the so this security breach.

Frankly, we consider Tiversa's "offer" as nothing short of blackmail. Also, the fact th Tiversa touts itself as MetLife's "vendor" also raises some questions about Tiversa' knowledge and access to this confidential information.

So far, Netxert has not met with the law enforcement authorities to complain about this security breach and Tiversa's tactics. However, soon Netxert will be obligated to (a) inform its employees (residing in several states) and (b) the FBI about this security breach. ***Before*** we take any of the above steps, we want to meet with MetLife's management and discuss these issues and try and work together to resolve this situation. However, time is of the essence in this matter. **We need to act fast**.

Again, I request you to make MetLife's legal personnel (and other necessary personnel) available for a face-to-face meeting on Monday. If you are not able to get everyone together on this short notice, please try and get your in-house lawyers available for a face-to-face meeting on Monday and the rest can join via teleconference. If not Monday, please schedule a meeting on Tuesday – but it is imperative that we have a face-to-face meeting. I do not want to keep discussing this matter via telephone back and forth.

I await your response. If you have any questions, please feel free to reach me on my cell (734-637-7112) over this weekend.

Thank you.

Ashish

ASHISH S. JOSHI
LORANDOS & ASSOCIATES
ATTORNEYS AT LAW
214 N. FOURTH AVENUE
ANN ARBOR, MI 48104
TEL: 734-327-5030
FAX: 734-327-5032
www.lorandoslaw.com

This e-mail is covered by the Electronic Communications Privacy Act, 18 U.S.C. Section 2510-2521 and is legally privileged. Unauthorized review, use, disclosure or distribution is strictly prohibited. The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and as such is privileged and confidential. If you are not the intended recipient, please contact the sender by reply e-mail, and destroy all copies of the original message. Unintended disclosure does not in any manner whatsoever waive the attorney-client privilege.

From: Michael Fradkin [mailto:mfradkin@metlife.com]

"a few days ago Netxert received a phone call from an agent of Tiversa, Inc."

"Tiversa offered to disclose this information, investigate the source of the breach and take remedial steps *if* Netxert agreed to retain Tiversa's services at $495/hour."

3. Boback Misrepresented Howard Schmidt's Role in Generating Business Contacts for Tiversa

Tiversa boasts an impressive board of advisors, a corporate governing body separate of the board of directors. The members of the advisory board include Howard Schmidt, General Wesley Clark, Maynard Webb, Larry Ponemon, Michael Dearing, Thomas Keevan, Lynn Reedy, and Patrick Gross.[140] The board purportedly provides "business" and "strategic guidance" to Tiversa.[141] Joel Adams praised the involvement of Tiversa's board. He stated, "Some companies use advisory boards as window dressing…The interaction is minimal, and that type of board isn't worth much. **Tiversa has been able to get its advisers to interact, to participate. When they walk about of a board meeting, they have to-do lists**."[142] Contrary to Adams' praise, however, according to Boback the advisory board met only once, in January 2006. [143]

Instead, Tiversa appears to use the advisory board primarily to solicit clientele. In a bulletin published by Morgan Lewis & Bockius, Boback stated, "when we considered advisers, we asked ourselves, 'Who can provide instructions? Whose credibility can we leverage to get where we need to be?'"[144] The article goes on to note, "Tiversa added the other [advisors], who became stepping stones to clients… and more."[145]

Howard Schmidt serves on Tiversa's board of advisors. During his tenure as advisory board member, he was appointed as the White House Cybersecurity Coordinator under President Obama.[146] Upon his appointment, Schmidt put the options he received from Tiversa into a blind trust. When asked by the Committee about Schmidt's role at Tiversa, Boback expressly denied that Schmidt helped generate business or introduce clients:

Q. Did Mr. Schmidt help generate any business for Tiversa?

A. I don't believe so.

Q. **Did Mr. Schmidt introduce you or anyone else at Tiversa to potential clients?**

A. **No.** [147]

Contrary to Boback's statement, the Committee has received extensive e-mail correspondence between Boback and Schmidt, where Schmidt systematically introduces Boback

---

[140] Tiversa Advisory Board, Tiversa, *available at* http://tiversa.com/about/advisors.html.
[141] Boback Tr. at 28.
[142] Evan Pattak, *Build a Better Board: See How a Solid Board of Directors Can Poise a Company for Success* 9, Getting It Done II, *available at* http://www.morganlewis.com/pubs/GettingItDone2BuildABetterBoard_TEQ2007i5.pdf (emphasis added) [hereinafter Pattack].
[143] Boback Tr. at 29.
[144] Pattack at 8..
[145] *Id.* (ellipsis in original).
[146] Macon Phillips, *Introducing the New Cybersecurity Coordinator*, The White House Blog (Dec. 22, 2009) http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.
[147] Boback Tr. at 41.

to potential clients and media contacts. In one e-mail to Schmidt, Boback praised him as "a lightning rod for business": [148]

"[Y]ou are clearly a lightning rod for business. I was (and am) extremely impressed by your extensive resume and experience which is what lead us to contact you for the advisor position."

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Tuesday, April 25, 2006 7:09 AM
To: howard@schmidt.org
Subject: RE: Demo of P2P issues

Howard:

This should be interesting. I see that Bob Sullivan had the exclusive [illegible] story. Given his background with Kazaa, he should quickly understand what we are talking about.

Also, the "Medical Passwords" file is a 36[illegible] that lists over 350 user ids/passwords for over 100 medical journal sites, clinical trials information site, etc. It is most likely someone in a large [illegible] setting keeping (or attempting to keep) the information for the use of these services (paid).

I also want to personally thank for the valuable time that you had spent with us during your visit to Pittsburgh. As I had mentioned during your visit, you are clearly a lightning rod for business. I was (and am) extremely impressed by your extensive resume and experience which is what lead us to contact you for the advisor position. After spending some time with you, I am even more impressed by the person behind such a resume and experience. It is an honor to work with you.

If you would like to send the topics of your upcoming engagements, we can have Captain PowerPoint put together various brief talking points sharing information and issues that we have seen related to your topics. I see that you have another ID theft talk mid-May at Georgia Tech. We can give some hard hitting points to share for this, if you think it would be helpful.

Hope all is well with you and your family, we'll talk soon.

Best Regards,
Bob

Tiversa played in active role in ensuring Schmidt could be an effective advocate. Chris Gormley, copying Boback, gave Schmidt explicit talking points on Tiversa's business model:[149]

[148] TIVERSA-OGR-0017729.
[149] TIVERSA-OGR-0017719.

From: Chris Gormley <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=CGORMLEY@tiversa.com>
Sent: Monday, May 1, 2006 12:40 AM
To: 'howard@schmidt.org'
Cc: Robert Boback <rboback@tiversa.com>
Subject: Slides
Attach: Howard043006.ppt

Howard,

Thank you for highlighting the problems we're addressing in your talks over the next 6 days. I've attached some information that may help you on Monday that is focused primarily on the problem in general. I put the files in a neutral file format. The example is a medical one, but it is one that had the least sanitization needed.

What I would like to do is to spend time after today (Monday) working up a more helpful set of slides / presentation to support your other talks this week. I envision the slides supporting two sections:

Section 1: Slides showing the problem in general

Section 2: Modules providing examples for:

1. ID Theft
2. Fraud
3. Regulatory Violations

To support Section 2, I have to sanitize some existing examples. Please let me know if ot[illegible] ill be helpful in section 2. Also, please let me know what I could do to make the slides I sent to you today more helpful including putting slides into templates tha[illegible] ur presentations.

Christopher L. Gormley
Chief Operating Officer
Tiversa, Inc.
The Leader in Information Containment Management
Office: 724-940-9030
Fax: 724-940-9033
Mobile: 724-991-3376

This e-mail message and any attachments contain confidential information from Tiversa, Inc. If you are not the intended recipient, you are hereby notified that disclosure, printing, copying, distribution, or the taking of any action in reliance on the contents of this electronic information is strictly prohibited. If you have received this e-mail message in error, please immediately notify the sender by reply message and then delete the electronic message and any attachments.

"Howard, Thank you for highlighting the problems we're addressing in your talks over the next six days. I've attached some information that may help you on Monday…"

Schmidt used these talking points to introduce Boback to potential clients. In June 2006, for example, Schmidt introduced Boback to FAA officials:[150]

From: Howard A. Schmidt <howard@cyber-security.us>
Sent: Saturday, June 3, 2006 5:19 PM
To: Michael F Brown <michael.f.brown@faa.gov>; Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>
Subject: FAA and Data Leakage

Mike,

It was great seeing you at the Aresight meeting and sorry I could not stick around for your presentation.

As I mentioned to you, I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal. What they have found is not just an errant document here and there but a systemic problem that is found in every sector.

To that end, I would like to introduce you to Bob Boback, the CEO and hopefully you can get a chance to see what they are doing up in Pittsburgh.

Best,
Howard

Sent via BlackBerry - short message and not spell checked.

"I have been working with Tiversa and thought that you would find the information that they have found on the P2P networks is unreal…

To that end, I would like to introduce you to Bob Boback…"

[150] TIVERSA-OGR-0017696.

During the same time, Schmidt introduced Boback to Paypal officials, joking that he hoped Paypal would not hold Schmidt's affiliation against Tiversa:[151]

"I would like to introduce you to Bob Boback…

During a recent call I had with Bob we were talking about the widespread issues around data leakage issues… and he mentioned that there were a number of PayPal related things that his folks had found."

From: Howard A. Schmidt <howard@cyber-security.u
Sent: Saturday, June 3, 2006 5:10 PM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINIS
Barrett <mbarrett@paypal.com>
Subject: "Data Leakage" and PayPal

Michael,

I hope this email finds you well and not too swamped. I would like to introduce you to Bob Boback, CEO of Tiversa a company I started working with on some homeland and defense security issues with.

During a recent call I had with Bob we were talking about the widespread issues around data leakage issues with P2P technology (eDonkey, limewire etc.) and he mentioned that there were a number of PayPal related things that his folks had found. I told him that I would let you know.

For full disclosure, I am their advisory board but hopefully you will not hold that against them. :)

Thanks and seeing what they have found, and continue to find, would be worth your time.

Best,
Howard
Sent via BlackBerry - short message and not spell checked.

"For full disclosure, I am their advisory board but hopefully you will not hold that against them. ☺"

Schmidt also approached Merrill Lynch on behalf of Tiversa, after Boback told him he had unsuccessfully tried to solicit the company:[152]

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Wednesday, April 19, 2006 9:29 AM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>; 'Basile, Anthony (IS&P)' <anthony_basile@aol.com>
Subject: Introduction as we talked about.

Hello Tony and Bob,

It was good talking with both of you recently and I hope this email finds you both well. Tony, as I mentioned I am on the advisory board of Tiversa and during a recent demonstration for some government related documents the discussion came up about data leakage and financial services. What Bob demonstrated for me was not an isolated document that was found but a widespread systemic leakage problem across ALL sectors, energy, telecom, transportation, financial etc. I think you mentioned that you had heard something about Tiversa but this is something that you have to see yourself to believe.

Thanks and I look forward to catching up next time I am in NY.

Best,
Howard

[151] TIVERSA-OGR-0017697.
[152] second TIVERSA-OGR-0017740

From: Howard A. Schmidt <howard@schmidt.org>
Sent: Tuesday, April 11, 2006 11:56 PM
To: Robert Boback <IMCEAEX-_O=TIVERSAINC_OU=FIRST+20ADMINISTRATIVE+20GROUP_CN=RECIPIENTS_CN=RBOBACK@tiversa.com>
Subject: RE: Merrill Lynch

(IN CONFIDENCE) I am working with them taking a look at their security program for their exec team. I will talk with Anthony Basile who has engaged me. Let me know if you want to send some samples.

Thanks
Howard

-----Original Message-----
From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Tuesday, April 11, 2006 3:02 PM
To: howard@schmidt.org
Subject: Re: Merrill Lynch

Hi Howard,
ML is one of the worst when it comes to leakage. We have made initial contact but have been stopped by a mid level IT individual named Swati Dutta Roy. They don't understand the problem. Any assistance that you can lend would be much appreciated.
Thanks
Bob

-----Original Message-----

From: "Howard A. Schmidt" <howard@cyber-security.us>
Subj: Merrill Lynch
Date: Tue Apr 11, 2006 11:44 am
Size: 227 bytes
To: "Robert Boback" <rboback@tiversa.com>

Hi Bob,

I have a consulting job with ML and as I talk with them I wanted to give them some insights into if they were leaking. Have you seen anything?

Thanks
Howard
Sent via BlackBerry - short message and not spell checked.

"(IN CONFIDENCE) I am working with them taking a look at their security program… I will talk with [ML official] who has engaged me."

"We have made initial contact but have been stopped by a mid level IT individual… Any assistance that you can lend would be much appreciated."

Tiversa also leveraged Schmidt's reputation for publicity. Schmidt contacted news outlets on Tiversa's behalf:[153]

From: Howard A. Schmidt [mailto:howard@schmidt.org]
Sent: Monday, April 24, 2006 11:19 PM
To: Robert Boback; 'Bob Sullivan (MSNBC-JV)'
Subject: Demo of P2P Issues

Bob (and Bob, MSNBC) ☺ ,

Bob Sullivan and I both spoke at an event with the AG for Ohio today on their ID Theft program. After the lunch, I talked with Bob about what you were doing and some of the really dangerous things that you showed me. I also explained to him that you did not want to alienate potential customers and that it would be counter productive to "report" on who had problems (everyone) but it might be a good way for Bob to raise the awareness. He did a story a while back around Kazzaa but I do not think he has seen anything like you showed me.

To that end, I would like to introduce you to each other to see what you can work out. Please let me know if there is anything I can do to help.

Best,
Howard

"I would like to introduce you to each other o see what you can work out."

[153] TIVERSA-OGR-0017729

The Committee found that, contrary to Boback's statements about Schmidt's role at Tiversa, Schmidt actively sought out contracts and potential clients for the company. This is yet another example of Boback providing false information during the course of this investigation.

4. Boback Misrepresented Information about Tiversa's Capabilities to Clients

According to a former Tiversa employee, Boback had a propensity to exaggerate, or even lie at times. Gormley stated, "the perception at least from what I remember internally was that there was a tendency to exaggerate or at least misrepresent… what was going on at the time."[154] Specifically, the feeling among some employees was that Boback's statements were "60 percent, you know, bullshit; 30 percent not true; and 10 percent truth, I guess, as far as like a representation of the facts."[155]

Gormley recalled a specific instance in which Boback misrepresented facts in meeting with a client:

> Q. When you say "third parties," do you mean potential clients?
>
> A. I remember the incidents. I mean, one was an existing investor, a limited partner within Adams Capital, came into the meeting, into a discussion, and **the number of employees and the revenues of our companies were overstated at the time**.
>
> The other was, well, to General Wesley Clark and Yahoo around **whether we were profitable or not**. And, again, you know, at the time, we were profitable for one quarter, but we weren't profitable for an entire year. I looked at that as misrepresenting that we're profitable, but you could argue that we were profitable for one quarter.
>
> There were also too many employees attributed to a potential acquirer named SecureWorks. That was later corrected, of course, in diligence, because you know how many employees you have, right?
>
> And those are some of the incidences I remember. And then -- so those are some -- I'm just trying to remember some of the other major areas.
>
> Q. Sir, did you ever confront Mr. Boback about these misrepresentations?

[154] Gormley Tr. at 131-32.
[155] *Id.* at 131, 136.

> A. Yeah, I mean, I told him, you can't do that, they're going to -- particularly in the case of potential acquirers, they're going to find out. I mean, let's not say that. We lose credibility in those instances.
>
> The case of this limited partner, the individual on the other end of the table was someone who friends of mine knew, so I felt personally at odds.
>
> Q. And this is the gentleman from Adams Capital?
>
> A. No, it's a limited partner, who was an investor in Adams Capital that came in to see essentially what Adams Capital was investing in. So, I mean, to me, the risks there were lower, because they had already invested. But we can't not state -- now, again, there's all different ways of viewing this. I mean, are you counting every single part-time potential person? Are you counting -- I mean, **but I recall it being an order of magnitude different**; it wasn't close.
>
> So that was one incidence -- set of instances that I remember.[156]

In another instance, Boback represented to a potential client that he had a close personal relationship with the FBI, implying retaliatory action if the client did not take action:

> **[I]n the discussion, Bob mentioned very lightly, but it stood out that he knows people at the local FBI office. And the veiled implication was that continue with monitoring, or else that FBI office might get wind of this.**[157]

During the course of its investigation, the Committee routinely found that it could not take information provided by Tiversa at face value—and statements made by former employees indicate that clients and potential clients could not do the same. The Committee found that Boback's statements about Tiversa's technological capabilities simply did not match what it found in the documents and testimony, Boback created a hostile work environment, withheld the nature of his relationship with Richard Wallace from the Committee, and created a culture at Tiversa based on a series of unseemly business practices. The Committee found that information provided by Tiversa—such as that on the Marine One leak—not only could not be verified, but at times appeared to be outright false. Given all the Committee has learned about Boback and Tiversa, the extent of its relationship with the Federal Trade Commission is extremely concerning.

V. Tiversa's Relationship with the Federal Trade Commission

[156] *Id.* at 27-29 (emphasis added).
[157] Gormley Tr. at 132-33 (emphasis added).

Tiversa's interactions with the FTC raise questions about the propriety of the relationship. Both Tiversa and the FTC have characterized the relationship as nominal. Overwhelming evidence produced to the Committee, however, demonstrates mutually-beneficial collaboration, wherein the FTC obtained information validated its regulatory authority, and Tiversa gained an ally in a powerful federal agency that provided actionable information that it exploited for monetary gain. Unfortunately, this relationship existed at the expense of good government.

The FTC accepted information from Tiversa through a shell organization without questioning the motives or reason for the third party, or, significantly, the veracity of the underlying information. The FTC's motives for blindly accepting this information are unclear.

In addition, Tiversa's involvement with LabMD, a medical testing laboratory based in Atlanta, Georgia, raises questions. Not only does LabMD's story offer a case study illustrating Tiversa's coercive business practices and relationship with the FTC, but information the Committee obtained shows that Boback lied about material information in the case, which ultimately led to the shuttering of LabMD.

According to a whistleblower, Tiversa withheld from the FTC information about its clients that had data breaches while providing information for companies that rejected the offer to buy Tiversa's services. According to the whistleblower, the FTC blindly trusted Tiversa's data and took only nominal steps to verify the information before embarking on the dissemination of warning letters and enforcement actions. Documents provided by the Federal Trade Commission also indicate the limited steps taken to verify information provided by Tiversa.

A. Tiversa misrepresented the extent of its relationship with the FTC to the Committee

On July 9, 2009, weeks before Tiversa testified before this Committee for the second time, the FTC sent a civil investigative demand to an entity Tiversa created called the Privacy Institute.[158] Tiversa responded promptly, passing documents and information about peer-to-peer breaches at nearly 100 companies through the Privacy Institute, which the Committee learned was created for the sole purpose of funneling information to the FTC pursuant to the CID. When the Committee asked Boback about Tiversa's relationship with the FTC, however, he painted a picture of a government agency bullying a small company. He testified:

> We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to—a small company having to be forced to provide information.
>
> **Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.**[159]

[158] Letter from Reginald Brown, Att'y, Tiversa to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (July 22, 2014).
[159] Boback Tr., at 43 (emphasis added).

Boback reiterated this sentiment by stating:

> And we felt -- frankly, as I mentioned, **we felt bullied or trapped to where we were saying I had no choice but to comply with something that was no benefit to Tiversa, was time-consuming, was costly to a small company**, kind of like I feel today.[160]

Boback asserted that Tiversa "denied" the FTC's request for information, and, under threat of a civil investigation demand (CID), Tiversa was compelled to provide information to the FTC.[161]

Consistent with his stated reluctance to cooperate with the agency, Boback described his contacts with the FTC as very limited. He testified he only knew one person at the FTC—Alain Sheer—and that he only interacted with Sheer on four occasions.[162] According to Boback, Sheer contacted him after the July 2009 Oversight hearing to set up a visit to Tiversa.[163] A second contact occurred when Sheer visited Tiversa in August 2009. Boback testified about the FTC's visit to Tiversa:

> So he came to Tiversa. They looked in our data center. They went in and said, "We'd like to talk about having" -- we met in our conference room and they said, "We'd like to talk about getting the copies of the information that you provided to House Oversight."
>
> They went into our data center to look at it. And he said, "I want these copy" -- "I need these printed out for us. I need these sent to us." And we said, "We don't send any information from our data center. Our data store is our data store. That is sacrosanct to us. So that's it." And they said, "Well, we're going to need to get this information, and we can use the CID, if necessary." We didn't know what a CID was. He said, "Civil investigative demand, similar to a subpoena. We're going to get the information." And we went, "Oh, no."[164]

Yet, by the time this meeting took place in August 2009, Tiversa had already received the CID. It is unclear why the FTC would threaten Tiversa with a CID a month after the CID was issued to the Privacy Institute.

Boback met with Sheer for the third time in Washington, D.C., after the Privacy Institute responded to the FTC's CID with information it in turn obtained from Tiversa.[165] Then,

---

[160] *Id.* at 218 (emphasis added).
[161] *Id.* at 43.
[162] *Id.* at 188 (Q: "What other attorneys at the FTC, besides Mr. Sheer, have you interacted with?" A: "There were two other attorneys at my deposition in November, but I don't recall their names… I don't know anyone at the—the only person I 'know' at the FTC is Mr. Sheer.").
[163] *Id.* at 184-85.
[164] *Id.* at 185-186.
[165] 186. As discussed below, representatives of the FTC do not recall meeting with Boback in Washington, D.C. It is not clear whether or not this meeting actually took place.

according to Boback, he did not have contact with Sheer until Sheer took his deposition in November 2013.[166] The fourth meeting occurred in June 2014—just before the Committee interviewed Boback.[167]

B. The FTC misrepresented the extent of its relationship with Tiversa to the Committee.

The FTC told the Committee that it had limited contact with Tiversa. Representatives from the Division of Privacy and Identity Protection of the Bureau of Consumer Protection told the Committee that the FTC first contacted Tiversa around the time of the July 2009 hearing.[168] FTC officials stated they found Tiversa to be a credible source of information, in large part, because of Boback's previous testimony before the House Oversight Committee.[169]

According to the FTC, after Tiversa sent the information responsive to the CID through the Privacy Institute, all subsequent contacts with Tiversa took the form of clarifying questions about the information provided by Tiversa.[170] Alain Sheer and Kristen Cohen made these calls.[171] As described above, FTC officials also recalled a meeting at Tiversa's offices in 2009, although they could not remember the details.[172] FTC officials did not recall any other meetings with Tiversa. Sheer in particular did not recall meeting with Tiversa in Washington, D.C.[173]

E-mails produced to the Committee—including from entities other than Tiversa—show a much more cooperative relationship between Tiversa and the FTC. Contrary to the assertions Boback made during his transcribed interview as well as those FTC officials made, documents show Tiversa's relationship with the FTC began in the fall of 2007. In October 2007, Boback participated in a conference call with FTC officials.[174] In December 2007, Boback provided documents to the FTC.[175] In June 2008, FTC attorney Carl Settlemyer thanked Boback for his "cooperation and insights into the area of inadvertent file sharing over P2P networks," and notified him that "confidential" information Tiversa provided to the FTC related to earlier Committee hearings on P2P networks would be produced to the Oversight Committee.[176] In

---

[166] *Id.*
[167] *Id.*
[168] Briefing by FTC officials to H. Comm. on Oversight & Gov't Reform Staff (Sept. 9, 2014) [hereinafter FTC Briefing].
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] *Id.*
[174] E-mail from Robert Boback to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Oct. 22, 2007 3:25 p.m.) [TIVERSA-OGR-0000071]; GoToMeeting Invitation—FTC Meeting 10:30 a.m. to 11:30 a.m.
[175] E-mail from Robert Boback, CEO, Tiversa to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Dec. 19, 2007 3:08 p.m.)[TIVERSA-OGR-0000065]; E-mail from Carl Settlemyer, Att'y, Fed. Trade Comm'n (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063].
[176] E-mail from Carl Settlemyer to Robert Boback (June 25, 2008 12:13 p.m.) [TIVERSA-OGR-0000063] (attached letter from Carl Settlemyer, Att'y, Fed. Trade Comm'n, to Robert Boback (June 25, 2008) [TIVERSA-OGR-0000064]).

March 2009, Boback again participated in a conference call with the FTC.[177] Days later, Boback bragged about the call: [178]

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, March 09, 2009 8:59 AM
To: Kline, Eric D.; Todd Davis
Subject: RE: Tiversa comparison

Todd,

I'm an in the office today if you want to discuss this after you have had a chance to review. I also wanted to give you an update on the great call that I had with the FTC on ID theft issues.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Personnel from the FTC's Division of Privacy and Identity Protection told the Committee that Tiversa's contacts with the FTC prior to the July 2009 hearing took place with a different division of the FTC.[179] Yet, Alain Sheer was included on e-mails with Boback requesting information about a recent Tiversa press release and scheduling the March 5, 2009, conference call[180]—the same call that Boback boasted about days later.

Tiversa's phone records are also telling of the company's relationship with the FTC. They indicate that Tiversa employees placed two phone calls to FTC attorney Laura Vandruff in June 2008, and that in the four months leading up to the July 2009 Oversight Committee hearing, Tiversa employees called Alain Sheer at his FTC office on 21 occasions.[181] Documents show that Boback was one of the FTC's main contacts at Tiversa prior to July 2009.

Regular phone calls between Tiversa and the FTC took place between August 2009, when Tiversa provided information to the FTC, and January 19, 2010, when the FTC sent letters to nearly all of the companies Tiversa turned over to the FTC. During these months, Tiversa

[177] E-mail from Robert Boback to Carl Settlemyer, Att'y, Fed. Trade Comm'n (Mar. 4, 2009 1:55 p.m.) [TIVERSA-OGR-0000052].
[178] E-mail from Robert Boback to Todd Davis, CEO of LifeLock, and Eric Kline (Mar. 9, 2009 8:59 a.m.) [LLOCK-OGR-000147]. Tiversa failed to produce this email to the Committee.
[179] FTC Briefing.
[180] *See* e-mail from Carl Settlemyer, Att'y, Fed. Trade Comm'n, to Robert Boback, CEO, Tiversa, Stacey Ferguson, Alain Sheer, & Richard Quaresima, Fed. Trade Comm'n (Mar. 4, 2009 5:25 p.m.) [TIVERSA-OGR-0000052-54].
[181] Consolidated Comm'ns, Invoice P7249409030020070816TIVERSA_INC [hereinafter Tiversa Phone Records].

employees called Alain Sheer 34 times.[182] The FTC represented to the Committee that only a handful of phone calls ever took place. Tiversa also represented to the Committee that the relationship between Tiversa and the FTC was nominal, and produced few documents indicating any ongoing contract with the FTC after July 2009, let alone this many interactions. The phone records stand in stark contrast to this assessment.

As discussed below, Tiversa used its advanced knowledge of FTC regulatory actions for its own commercial gain.

C. The FTC failed to question Tiversa's creation of a dubious shell organization, the Privacy Institute, to funnel information to the FTC

Despite the friendly relationship between Tiversa and the FTC, Tiversa asked the FTC to accept documents from a company it created for the sole purpose of responding to the FTC—the Privacy Institute. The certificate of incorporation was filed in Delaware on June 3, 2009.[183] Boback testified about Tiversa's purpose in creating the Privacy Institute:

> Q. Mr. Boback, what is The Privacy Institute?
>
> A. Privacy Institute is an organization our lawyers set up.
>
> Q. For what purpose?
>
> A. Well, was it originally? I mean, it was –
>
> Q. For what purpose was it set up?
>
> A. Right. It was set up to provide some separation from Tiversa from getting a civil investigative demand at Tiversa, primarily. And, secondarily, it was going to be used as a nonprofit, potentially, but it never did manifest.[184]

* * *

[182] *Id.*
[183] Sec'y of State, State of Del., Div. of Corps., Certificate of Incorporation, No. 4694728 (June 3, 2009) . [hereinafter Certificate of Incorporation]. The Privacy Institute was dissolved on June 18, 2013. On the certificate of dissolution, the address for Brian Tarquinio is that of Boback's uncle. In a deposition taken just days after the Committee's transcribed interview, Boback testified that he did not know why his uncle's address was used on the certificate of dissolution. Deposition of Robert Boback, In the matter of LabMD, No. 9357 (June 7, 2014) at 38. Tarquinio also testified that he did not know why the address of Boback's uncle was listed as his own on this document. Tarquinio Tr. at 23-24. Upon learning this information, the Committee asked Boback why the address of his uncle was used on this document. Letter from Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform, to Robert Boback, CEO, Tiversa (June 23, 2014). One month later, Boback, through his counsel, answered that he did not recall. Letter from Reginald Brown, Att'y, Tiversa, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight & Gov't Reform (July 23, 2014).
[184] Boback Tr., at 42.

A. I don't know if it was their idea or our idea. We wanted to create separation, as we felt we were being bullied by the FTC into having to provide information to -- a small company having to be forced to provide information.

Because in July of 2009, I testified before this committee and then I was bullied by the FTC the very following month, in my opinion, in providing that information.

When we denied providing them information, all of a sudden we were told that, "You have no -- you have no right to deny it, and here's a civil investigative demand that is coming for this."

And we talked to them and said, "We are in acquisition talks at Tiversa and the last thing we want to have is some Federal subpoena or civil investigative demand coming to us."
So our lawyers, in talking to the FTC, they said, "Fine. We'll send this civil investigative demand to this other company, this Privacy Institute, and do it that way."[185]

In the same interview, Boback stressed again that the "singular purpose" of the Privacy Institute was to maintain distance between Tiversa and the FTC's CID. Boback stated:

Q. How would you describe the relationship between the Privacy Institute and Tiversa?

A. It was one singular purpose that was to make sure or try to do whatever we could so that the FTC did not send a CID, the civil investigative demand, to Tiversa. And that was the only option that our attorneys came up with and the FTC was okay with. So -- or, I don't know if they were okay with it. If they were okay with it, they did it.[186]

Boback asked Brian Tarquinio, his financial advisor, to be the President of the Privacy Institute. Tarquinio accepted the requested as a "favor" to Boback.[187] Tarquinio had a different understanding of the purpose of the Privacy Institute. Tarquinio stated:

Q. Could you describe for us what the Privacy Institute is?

A. I don't think it's anything at this point.

Q. How about what it was?

---

[185] *Id*. at 43.
[186] *Id*. at 48.
[187] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Brian Tarquinio (Sept. 5, 2014), at 57 [hereinafter Tarquinio Tr.].

A. Sure. To my best recollection, **it was an entity that was established to take bids for either part or all of Tiversa if a company wanted to purchase them.**[188]

* * *

A. Sure. My recollection is **it was set up because at the time there were companies that were interested in potentially purchasing Tiversa, and it would be a separate entity to take those bids.**[189]

Tarquinio's understanding of the purpose of the Privacy Institute came directly from Boback:

[Att'y] Why don't you just explain how it came to your attention, what your involvement was, and then they'll have follow-ups.

A. Sure. Mr. Boback came to me and said, we have a company, and at the time I believe it was LifeLock, who was interested in purchasing, you know, some part of Tiversa, which I was aware of. **And he said, we want to create an entity separate from Tiversa to accept those bids, so it is not on our corporate side of everything.** We would like to see if you would be, you know, the head of the Privacy Institute. And as a friend, it seemed pretty reasonable. I said to him, sure, if I get approval [from my employer], fine, glad to.[190]

According to Tarquinio, Boback did not inform Tarquinio that the Privacy Institute was set up to transmit information to the FTC. In fact, Boback did not even mention the involvement of the FTC to Tarquinio. Tarquinio stated:

Q. Concurrent with your involvement in the Privacy Institute, were you told that the creation of the Privacy Institute had anything to do with the FTC's interactions with Tiversa?

A. At that time, no. I had no knowledge of the FTC's interaction with Tiversa.[191]

Tarquinio had no knowledge that the Privacy Institute had ever transmitted information to any government entity,[192] and only recently learned of the Privacy Institute's connection to the FTC:

---

[188] *Id.* at 16.
[189] *Id.* at 17.
[190] *Id.* at 20.
[191] *Id.* at 21.
[192] *Id.* at 22.

Q. At what point in time did you learn that the Privacy Institute was somehow connected to the FTC? Was it during the course of your preparation for today?

A. Yes, ma'am.[193]

Tarquinio's testimony contradicts Boback's explanation of the Privacy Institute's creation, and raises questions regarding the true purpose and activities of the Institute, which remain unknown.

Regardless of the reasons that Boback created the Privacy Institute, it is not in dispute that Tiversa used the Privacy Institute to send information to the FTC. The FTC did not question Tiversa's use of the Privacy Institute, and did not know that the Privacy Institute was set up solely to respond to the FTC's request for information.[194] FTC officials clearly knew that the information was, in fact, coming from Tiversa, despite the use of the Privacy Institute.[195] The FTC admitted that the use of Tiversa's information was unusual relative to standard agency operating procedures for enforcement measures.[196]

FTC officials relied heavily on Tiversa's "credible" reputation in "self-verifying" the produced information.[197] The FTC explained to the Committee the steps it took in "self-verifying" the information:

- Tiversa, through the Privacy Institute, certified the information provided under penalty of perjury.
- FTC employees looked up the IP addresses provided by Tiversa to determine if the IP address was affiliated with the company.
- FTC employees looked at the metadata of the documents, when provided, to determine the author or the document.
- FTC employees performed "some" searches on the peer-to-peer networks, both for company names and specific documents. The FTC independently found only one of the files Tiversa submitted on the peer-to-peer network.[198]

Ultimately, outside of some minimal work verifying IP addresses and looking at metadata, the FTC relied entirely on the list of companies and documents Tiversa provided. Of the 88 companies Tiversa submitted to the FTC, the agency sent warning letters to 63 companies, and opened investigations into 9 companies.[199] The FTC also issued a press release on the letters

[193] *Id.* at 22-23.
[194] FTC Briefing.
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] [FTC_PROD16732-16964].

and received considerable media exposure for its new work related to data security. According to the FTC, this was the only time it obtained information from Tiversa.

The FTC further explained that it only needs "reason to believe" that a company is failing to adhere to appropriate data security standards before sending a warning letter or issuing a complaint. The agency was comfortable with the extent of the "self-verifying" steps it took before sending warning letters and opening investigations into nearly 100 companies. The FTC categorically denied to the Committee that it gave Tiversa notice that it would be using the information in letters to companies. Documents the Committee obtained during the course of this investigation suggest otherwise.

D. Tiversa manipulated advanced, non-public, knowledge of FTC regulatory actions for profit

Tiversa had advanced knowledge that the FTC intended to pursue regulatory actions against many of the companies it turned over to the Privacy Institute in response to the CID. FTC officials maintained to the Committee that no one at the FTC provided advance information of the January 2010 regulatory actions to Tiversa.[200] Tiversa did not produce the overwhelming majority of the documents indicating Tiversa's intention to profit off the FTC's actions. Tiversa failed to produce these documents despite the fact that they were clearly responsive to both the original subpoena, and the search terms provided by Committee staff.[201] The Committee obtained these documents from other sources.

Armed with non-public knowledge of these impending actions, Tiversa maneuvered to position itself to profit from the FTC's actions. In the fall of 2009, Boback began working with LifeLock, a major partner of Tiversa and Tiversa's largest source of income, to send letters to the companies that would be contacted by the FTC—the very companies that Tiversa turned over to the FTC. In October 2009, Boback e-mailed senior LifeLock executives about the impending FTC investigations:[202]

[200] FTC Briefing..
[201] Subpoena from H. Comm on Oversight & Gov't Reform to Tiversa, Inc. (June 3, 2014). The subpoena requires production of "all documents and communications referring or relating to work Tiversa, Inc. performed for the Federal Trade Commission. *Id*. The Committee further provided the search terms "FTC" and "Federal /2 trade /2 commission".
[202] E-mail from Robert Boback to Mike Prusinski, Todd Davis, and Clarissa Cerda (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, October 26, 2009 7:37 AM
To: Mike Prusinski; Todd Davis; Clarissa Cerda
Subject: RE: 60 minutes

As soon as I get the OK from the FBI, we will be off an running. We have some huge rings that we are tracking right now but I can't discuss as they are open investigations. We hired a new guy that came from the Secret Service to help us address these crimes.

Also, there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next. Should be interesting...

And....the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P. This is a huge increase for them since they have only prosecuted 25 cases since 2001. The Washington Post is already planning on writing a big expose on that and they plan to name companies in an effort to shame them into properly addressing this for the individuals exposed.....ie buy LL. :-) There are about 600-700K individuals on those lists, therefore if we time things right, LL can have a huge upswing in members AND LL will have pricing power over the companies that leaked the information. Since LL is still the only company that can offer P2P remediation, you will be the only choice for the solution. :-)

I saw the settlement of the Experian suit.....they mus[illegible] seen that Todd on the stand and Clarissa on a cross examination would not be beneficial to their [illegible]iability.....

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P"

The "100 or so companies that have breached consumers [*sic*] information via P2P" were the same companies that Tiversa itself reported to the FTC. Boback further explained that the *Washington Post* planned to "shame" companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit.[203]

Boback's scheme to profit from the FTC investigations took shape in the coming weeks. In early October 2009, Boback advised LifeLock that "the FTC letters did not go out yet so the companies will not know what you are talking about……yet."[204] He further advised that LifeLock should "be solo" and "suggest Tiversa if asked by the company."[205]

[203] *Id*.
[204] E-mail from Robert Boback to Anthony Hesano, LifeLock (Oct. 6, 2009 8:40 a.m.) [LLOCK-OGR-0001929]. Tiversa failed to produce this e-mail to the Committee.
[205] *Id*.

----- Original Message -----
From: Robert Boback <rboback@tiversa.com>
To: Anthony Hesano
Sent: Tue Oct 06 08:40:21 2009
Subject: RE: FTC letter

I agree with your approach. The FTC letters did not go out yet so the companies will not know what you will be talking about.....yet. I think that it LL should be solo on this.....you could always suggest Tiversa if asked by the company. :-)

It was great to catch up with you and Ally as w I understand that Jacque is in town this week. Brian is a totally straight up guy that lutely not try anything out of line, or even close to any line.....and I mean that.

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"The FTC letters did not go out yet so the companies will not know what you will be talking about...yet. I that that… LL should be solo on this… you could always suggest Tiversa if asked by the company. ☺"

The following month, Tiversa and LifeLock's strategy with respect to the as-yet-unannounced FTC investigations became clear. In a November 3, 2009, e-mail, a LifeLock employee stated that he "spoke with Bob" about repositioning the letter.[206] He described the attached version as one that will "get the response we are looking for without overplaying our cards." Another LifeLock employee responded, stating, "As mentioned, Clarissa has stopped this pending the FTC but our strategy is to send a letter similar to the one outline[d] along with the breach brochure."[207] A later e-mail describes the revised strategy:[208]

[206] E-mail from Gary Woods to Steve McGrady, Eric Warbasse, and Chris Miller (Nov. 3, 2009, 10:35 a.m.) [LLOCK-OGR-0002044].
[207] E-mail from Steve McGrady to Gary Woods, Eric Warbasse, Chris Miller, and Austin Colcord (Nov. 3, 2009 12:00 p.m.) [LLOCK-OGR-0002043-2044].
[208] E-mail from Gary Woods to Austin Colcord and Chris Miller (Nov. 3, 2009 2:25 p.m.) [LLOCK-OGR-0002043].

"Key points:

- **No FTC reference**
- **No Tiversa reference**
- **No P2P reference"**

From: Gary Woods
Sent: Tuesday, November 03, 2009 2:25 PM
To: Austin Colcord; Chris Miller
Cc: Anthony Hesano; Eric Warbasse; Steve McGrady
Subject: FW: LifeLock Breach Services - intro letter

Austin & Chris

I re-wrote the letter and believe it is on target – and generic enough that Legal is not going to have any issue. I spoke with Eric & Austin about it and now I just need Chris to have Legal approve the verbiage.

Key points:
- No FTC reference
- No Tiversa reference
- No P2P reference

This is solely to make these accounts aware of LifeLock so when they fully realize the need to respond to a data breach – they think of LifeLock first and have our contact information to reach out and partner with us. I'm sure based on discussions with Bob that Tiversa will also be involved with these accounts and will reinforce their need to provide a LL solution in their breach compliance letter to affected individuals.

Thanks for your help,

Gary

As discussed, the draft letter, as provided to Boback on November 3, 2009, contains no reference to the FTC, no reference to Tiversa, and no reference to the peer-to-peer networks.[209]

On February 22, 2010, the FTC announced that it notified "almost 100 organizations" about data breaches that occurred on peer-to-peer file sharing networks, and opened non-public investigations into several other companies.[210] Boback sent the link to executives at LifeLock:[211]

From: Robert Boback
To: Gary Woods; Todd Davis; Mike Prusinski
Sent: Mon Feb 22 09:30:18 2010
Subject: FTC press release
Guys,

Check out this link.....then ask yourself who knows what's going on?!?!?!?! :-)

http://www.ftc.gov/opa/2010/02/p2palert.shtm

Best,
Bob

Robert Boback
Chief Executive Officer

1

[209] Draft Letter, LifeLock (undated) [LLOCK-OGR-0002045].
[210] Press Release, FTC, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* http://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe
[211] E-mail from Robert Boback to Gary Woods, Todd Davis, and Mike Prusinski (Feb. 22, 2010 9:30 a.m.) [LLOCK-OGR-0002375].

LifeLock responded, "Once again you guys are at the top of the food chain. Any problem with us pushing this with media and using you?"[212] Boback promptly replied, "No problem."[213]

In an interview with *Computerworld* days after the FTC press release, Boback stated, "We were happy to see that the FTC [has] finally started recognizing that P2P is a main source for criminals to gain access to consumer's personally identifiable information for ID theft and fraud."[214] Boback further stated that complying with the FTC's request for information could be "extensive and cumbersome," and that 14 of the companies the FTC contacted had already contacted Tiversa for help.[215] The *Computerworld* article does not mention that Tiversa acted as the primary source for the FTC's enforcement actions announced in February 2010.[216]

When asked about the propriety of Tiversa seeking to profit from its dealing with the FTC, FTC attorney Alain Sheer stated that it was routine for the FTC to make clear to third parties that the information was not public.

> Q. In the course of your interactions with Tiversa in the pre-complaint period, did you or one of your colleagues ever tell Tiversa not to discuss the conversations that the FTC and Tiversa were having with third parties?
>
> A. It is routine for Commission staff to ask entities that are providing information to keep the information confidential.
>
> Q. Do you recall making that specific request to Tiversa? A I don't recall it. Q It would've been your general practice or your colleagues' general practice to make that request? A Yes.[217]

Sheer further testified that he was unaware of Tiversa seeking to profit off of the information provided to the FTC until shown documents produced to the Committee and that the scheme with Lifelock was concerning.

> Q. Does it concern you that Mr. Boback seems to have obtained some sort of information about what the FTC planned to do as early as October 26, 2009?
>
> A. The company provided information about roughly 100 companies when they looked at it. They are well aware of what it is they gave to us. So is it a concern?

---

[212] E-mail from Mike Prusinski to Robert Boback (Feb. 22, 2010 11:47 a.m.) [LLOCK-OGR-0002375].
[213] E-mail from Robert Boback to Mike Prusinski (Feb. 22, 2010 10:00 a.m.) [LLOCK-OGR-002375].
[214] Jaikumar Vijayan, *FTC Questions Firms Being Probed for P2P Breaches*, TECHWORLD (Feb. 26, 2010), http://news.techworld.com/security/3213712/ftc-questions-firms-being-probed-for-p2p-breaches/?olo=rss
[215] *Id*.
[216] Tiversa informed the Committee that it had prior business relationships with 11 companies whose information was included in response to the CID. This conflicts with statements Boback made in the *Computerworld* interview that "14 of the companies contacted over the leaks have already contacted Tiversa for help" and that "all but two of those have CIDs." Not only is the number of companies with contracts with Tiversa inconsistent, but many of the companies that received CIDs from the FTC did not, in fact, have contracts with Tiversa.
[217] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm'n, Transcript at 94 (Oct. 9, 2014) (hereinafter Sheer Tr.).

> Yes. I'd like it to be kept confidential. That's the point of asking for it to be kept confidential.[218]

Troublingly, despite Tiversa's close relationship with Lifelock, a company that was itself the subject of an FTC investigation, Sheer stated that he was unaware of the relationship between Lifelock and Tiversa before being informed of it by Committee staff in a transcribed interview.

> Q. Are you aware of Tiversa and LifeLock having a -- having a business relationship -- I guess, what is your awareness of Tiversa and LifeLock's business relationship?
>
> A. I don't know that they have a business relationship other than the statement that was made in the -- in the email that you -- that you presented earlier.
>
> Q. Okay. Was the email I presented earlier the first you'd heard of Tiversa and LifeLock having any relationship?
>
> A. Yes.[219]

Boback could not have known the details of the FTC's investigations—including the timing of the letters, which constituted pre-decisional information about pending non-public government actions —without some sort of inside knowledge about the FTC's enforcement plans. While the Committee's investigation has not yet identified the source of the Tiversa's information about the FTC actions, it is clear that Tiversa and the FTC had a mutually beneficial relationship. The FTC used Tiversa as the source of convenient information used to initiate enforcement actions, and Tiversa used the FTC to in further pursuing the company's coercive business practices.

E. Information provided by Tiversa formed the basis of the FTC's case against LabMD

Documents produced to the Committee show that in an effort to generate business, Tiversa repeatedly sought to coerce companies to purchase its services. Tiversa's methods have ranged from contacting a company about a leak but failing to provide anywhere close to full information, to referring nearly 100 companies to the FTC. The Committee has spoken to numerous companies on the list Tiversa provided to the FTC—not one of the companies the Committee contacted had entered into a contract with Tiversa. One such business tangled in Tiversa's web was LabMD.[220] In January 2014, it closed its laboratory operations because of costs incurred by its dealings with Tiversa and the FTC.[221]

---

[218] *Id*. at 107.
[219] *Id*. at 170.
[220] *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight Gov't Reform*, 113th Cong., at 18 (July 24, 2014) [hereinafter Daugherty Testimony] (statement of Michael Daugherty, CEO of LabMD).
[221] *Id*. at 72.

According to Boback, Tiversa downloaded a file containing patients' personally identifiable health information in February 2008.[222] Tiversa determined that the downloaded file likely belonged to LabMD, and contacted the company in May 2008. Tiversa provided LabMD with a copy of the file, but would not provide the IP address or other information unless LabMD agreed to purchase Tiversa's services.[223]

Tiversa referred LabMD to the FTC as one of the companies listed in the spreadsheet as responsive to the FTC's CID. The FTC, in turn, sent a complaint letter to LabMD. The FTC then initiated an administrative enforcement action against LabMD for unfair and deceptive business practices.

Among the information Tiversa gave to the FTC regarding LabMD was the IP address that was the source of the leak. The origin of the IP address from where the LabMD document was pulled was a matter of contention in the litigation between LabMD and Tiversa. On numerous occasions, Boback maintained that Tiversa had pulled the LabMD document from an IP address in San Diego, California:

> Q. Going back to CX 21. Is this the initial disclosure source?
>
> A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.
>
> Q. When did Tiversa download CX 10?
>
> A. I believe it was in February of 2008.
>
> Q. Has CX 10 changed in any way since Tiversa downloaded it?
>
> A. No.[224]

When asked about the Georgia IP address, Boback denied downloading the information from there:

> Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?
>
> A. That, if I recall, is an IP address that resolves in Atlanta, Georgia.

* * *

[222] Fed. Trade Comm'n, Deposition of Robert Boback, In the Matter of LabMD, Inc. 25-26 (Nov. 21, 2013) [hereinafter Boback FTC Deposition].
[223] Daugherty Testimony, at 19.
[224] Boback FTC Deposition, at 25-26.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.[225]

In an internal e-mail dated almost three months before the deposition and never produced to the FTC, however, Boback stated that Tiversa downloaded the LabMD file while working for a client. He stated, "The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. This statement, made by Boback in September 2013, fundamentally calls into question his claim that Tiversa never downloaded the LabMD file from the IP address in Georgia.[226]

From: Robert Boback <rboback@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a pla against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is base in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa "hacked" his company in an effort to get a file containing nearly 9,000 patient's SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or Information security which is what caused him to think that he was "hacked" and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he woul not do business with Tiversa to remediate the problem, that Tiversa "kicked the file over to the feds [FTC]" (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him "great harm" due to the widespread "government shakedown of small business." He claimed that Tiversa was attempting to extort money from him to "answer his questions" as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory o the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his "true story" was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as "Batman" (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his "true story" about how the government is out to "get" small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, "Devil inside the Beltway" is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a "name" for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this "dolphin in the tuna net"....for example, if we were looking for "Goldman Sachs" and our system finds a file with the term "Goldman" in it. The file may have the name "Henry Goldman" but our system just saw "Goldman" and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company [illegible] inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for addition[illegible]mation that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about $15K. After hearing this, h[illegible] send him the SOW for the services. 2-3 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he [illegible] (re: SOW) and he told me never to contact him again with no further explanation. We didn't.

"The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."

[225] Boback FTC Deposition, at 41-42.
[226] E-mail from Robert Boback to Dan Kopchak and Molly Trunzo (Sept. 5, 2013 3:20 p.m.) ("The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located.") [TIVERSA-OGR-0028866].

Further, the initial report that Tiversa provided to a client about the LabMD document stated that the company first "observed" the LabMD file in San Diego, California on August 5, 2008.[227] Tiversa could not have downloaded the LabMD file from an IP address in San Diego in February 2008 if it did not even observe the file at this IP address until August 2008.

In light of the information uncovered by the Committee's investigation, it appears the FTC was misled as to how Tiversa came to possess LabMD's file, which has been a material fact in the litigation of the enforcement action. Mr. Sheer testified that, contrary to information provided to the Committee, the FTC had never been told that the file was originally downloaded in Atlanta, Georgia.

> Q. Did anyone from Tiversa ever tell you that they first downloaded the file from Atlanta, Georgia, and not from San Diego, California?
>
> A That wasn't what the testimony was.
>
> Q Have you seen any documents during the course of your investigation indicating that Tiversa first downloaded the document from Atlanta, Georgia, and not from San Diego, as it testified to the FTC?
>
> A. Not that I am aware of.[228]

The discrepancies in the accounts of Tiversa's downloading of the LabMD file and the information provided to the FTC call into question the FTC's processes for relying on third-party sources and integrity of its actions against LabMD.

Finally, Tiversa recently performed another forensic analysis on the LabMD file after inexplicably telling the FTC that Tiversa had provided misinformation about the case.[229] This analysis stated that the LabMD file was disclosed by an IP address in Atlanta, Georgia between March 7, 2007, and February 25, 2008.[230] Yet, this information does not comport with the facts of the case. When Tiversa contacted LabMD on [DATE], LabMD performed an investigation and found that a billing manager's computer had LimeWire P2P software installed, and was sharing the LabMD file. Why did Tiversa's systems determine that the Georgia IP ceased to share the LabMD file in late February 2008, when LabMD's own investigation determined that the file was still being shared months later? Why wasn't this information captured by Tiversa's technology?

All of this information not only calls into question Tiversa's technological capabilities, but also Tiversa's claim that it never downloaded the LabMD file from a Georgia IP address – a

[227] Tiversa Forensic Investigative Report for Ticket #CIG00081 (Aug. 12, 2008) [TIVERSA-OGR-0017461-17465].
[228] Sheer Tr. at 151.
[229] Boback Tr., at 130.
[230] Tiversa Forensic Investigation Report – LABMD0001 (June 4, 2014) [TIVERSA-OGR-0017467-17482].

critical fact in the case against LabMD. As described above, Tiversa's Eagle Vision software purportedly downloads a document every time it hits on a search term. While the software will not download a document from the same IP address twice, it will download the same file from different IP addresses, which indicates the spread of the document. To the Committee's knowledge, Tiversa has not explained in this investigation or other legal proceedings why the software did not download the file from the Georgia IP address. Even assuming that Tiversa was unable to download a file due to technological problems (for example, because the peer-to-peer user signed off while Tiversa was downloading the file), then its software would make another attempt to download the file the next time it was available. Boback has testified that the LabMD file was available on the peer-to-peer network. Either the software does not download a relevant file each time it spreads to a new IP address, which fundamentally calls into question Tiversa's capabilities, or Tiversa did download the LabMD file from the Georgia IP address, a key point in the FTC proceeding.

There is little reason to doubt Boback's statements made to two Tiversa employees—the e-mail clearly shows Boback describing Tiversa's role in the FTC's LabMD enforcement action. Why Boback wrote this e-mail is unknown. It is possible he wanted to make sure he had his facts straight before he was deposed in the FTC matter. Further, Dan Kopchak, to whom Boback sent the e-mail, replied with a draft that made minor edits to the narrative but did not change or question the statement that the IP originated in Georgia.[231] Therefore, information the Committee obtained shows that Boback's testimony that source of the IP address came from San Diego is not true. Boback's conflicting statements have broad implications for the future of litigation between LabMD and Tiversa, and calls into question other information he has provided to the FTC.

In short, LabMD witnessed both Tiversa's manipulative business practices and Tiversa's close relationship with the FTC. Evidence produced to the Committee shows that the FTC notified Tiversa of its investigatory schedule, so that Tiversa knew when the Commission would issue complaint letters and act accordingly.

A whistleblower's account of the LabMD saga suggests that the patient data file was only found emanating from a LabMD computer in Atlanta, GA. The whistleblower demonstrated for the committee in tremendous detail how he found IP addresses associated with known identify thieves (also referred to as "information concentrators") and created documents later provided to the FTC showing that the file was in the possession of known-identity thieves when in fact there is no evidence to suggest it was downloaded by anyone other than Tiversa. The reason for forging the IP addresses, according to the whistleblower, was to assist the FTC in showing that P2P networks were responsible for data breaches that resulted in likely harm, not just the exposure of the information from the source computer which could have been easily remedied.

[231] E-mail from Dan Kopchak to Robert Boback (Sept. 5, 2013 4:01 p.m.) (revisions from the earlier draft included changes such as "was" to "were;" qualifying "understanding of P2P Information security" to "*may have* caused him to think that he was 'hacked' and which *apparently* has resulted in his widespread government conspiracy theory that followed;" the deletion of "Needless to say," etc.) [TIVERSA-OGR-0025706].

Ultimately, LabMD began to wind down operations in January 2014 as a result of the FTC enforcement action.[232]

F. Tiversa withheld documents from the FTC

The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

1. Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.[233] Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.[234]

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."[235] In a transcribed interview, Alain Sheer, an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

> Q. This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?
>
> A. I am not sure what your question is.
>
> Q. Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?

[232] Michael J. Daugherty, *FTC Actions Force LabMD to Wind Down Operations* (Jan. 28, 2014), http://michaeljdaugherty.com/2014/01/29/labmd-winds-operations/.
[233] Boback Tr. at 42.
[234] *See* Tiversa, Industry Outlook, Government/Law Enforcement, *available at* http://tiversa.com/explore/industry/gov (last visited Nov. 21, 2014); Boback Tr. at 42-43.
[235] Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

A. Not that I am aware of.[236]

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

Q. What is the significance of the IP address, which is 68.107.85.250?

A. That would be the IP address that we downloaded the file from, I believe.

Q. Going back to CX 21. Is this the initial disclosure source?

A. If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q. When did Tiversa download [the LabMD file]?

A. I believe it was in February of 2008.[237]

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.[238] In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A. That, if I recall, is an IP address that resolves to Atlanta, Georgia.

Q. Is that the initial disclosure source?

A. We believe that it is the initial disclosure source, yes.

---

[236] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer at 147 (Oct. 9, 2014).
[237] In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].
[238] Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").

Q. And what is that based on?

A. The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.

* * *

Q. So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?

A. We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.

Q. What other information do you have about 64.190.82.42?

A. I have no other information. I never downloaded the file from them. They only responded to the hash match.[239]

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

2. Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, "[a]ll documents and communications referring or relating to LabMD, Inc."[240] This request was very similar to the FTC's request for "all documents related to LabMD."[241] Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

[239] Boback Nov. 2013 FTC Tr. at 41.
[240] H. Comm. on Oversight & Gov't Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).
[241] Tiversa FTC Subpoena.

An internal Tiversa document entitled "Incident Record Form," dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa's production to the Committee.[242] This document states that on April 18, 2008, Tiversa detected a file "disclosed by what appears to be a potential provider of services for CIGNA."[243] The Incident Record described the document as a "single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients," and explained that "[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source."[244] The name of the file was "insuranceaging_6.05.071.pdf," which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.[245] Upon learning about the file, CIGNA, a Tiversa client, "asked Tiversa to perform Forensic Investigation activities" on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.[246]

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the "original source" of the Incident Record Form.[247] A spread analysis included in the August 2008 forensic report stated that the file had been "observed by Tiversa at additional IP addresses" but made clear that Tiversa had not downloaded the file from either additional source because of "network constraint and/or user behavior."[248] Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback's testimony that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.[249] Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.[250] Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again,

---

[242] Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).
[243] *Id*.
[244] *Id*. (emphasis added).
[245] *Id*.
[246] Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase "forensic report" to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.
[247] *Id*.
[248] *Id*.
[249] The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was "most likely an IP shift from the original disclosing source."
[250] *Id*.

the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. <u>The IP of the download was found to be in Georgia,</u> which after a Google search, is where we found LabMD's office to be located."[251]

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."[252] Tiversa withheld these relevant documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's

[251] E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].
[252] Tiversa FTC Subpoena.

system names files.[253] If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

3. Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008 from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008 until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007 and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

4. Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.[254] Chief Administrative Law Judge D. Michael

[253] Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose."[255] Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.[256]

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback's June 2013 deposition.

Tiversa's failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa's credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa's discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide.

VI. *Tiversa's Involvement with House Ethics Committee Report Leak*

A. The *Washington Post* breaks the story

On October 29, 2009, the *Washington Post* reported that the U.S. House of Representatives Committee on Ethics was investigating the activities of "more than 30

[254] Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014), http://www.ftc.gov/system/files/documents/cases/572572.pdf [hereinafter Notice of Information].
[255] *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/.
[256] Notice of Information at 4.

lawmakers and several aides."[257] The *Post* based its reporting on a "confidential House ethics committee [*sic*] report" inadvertently disclosed on a peer-to-peer network.[258] "A source not connected to the congressional investigations" provided the document to the *Washington Post*.[259] The Ethics Committee stated that a junior staffer released the document after installing peer-to-peer software on a home computer.[260] The staffer was subsequently fired.[261]

The *Washington Post*'s story indicated that the leaked "Committee on Standards Weekly Summary Report" provided summaries of non-public ethics investigations of nineteen lawmakers and several staff members, as well as non-public investigations into fourteen additional lawmakers undertaken by the Office of Congressional Ethics.[262]

The same day that the *Washington Post* published its story, Chairwoman Zoe Lofgren made a brief statement about the leak on the House floor.[263] News of the leak prompted a review of the House's information systems to determine whether there had been any breach beyond the inadvertent leak of the Ethics Committee document on the peer-to-peer network.

Tiversa began providing written information about the leak to the House Ethics Committee in early November 2009, after the *Washington Post* broke the story. Documents produced by Tiversa, however, show that Boback was aware of the leak and its significance more than a week before the story was published. On October 20, 2009, a Tiversa analyst e-mailed Boback the name, resume, and Facebook profile picture of a House Ethics Committee staffer.[264] The subject line of the e-mail read, "US Rep Ethics Doc Leaker."[265] On October 26, 2009, four days before the *Washington Post* published its story, Boback wrote an e-mail to executives at LifeLock. He stated:[266]

---

[257] Ellen Nakashima & Paul Kane, *Dozens in Congress Under Ethics Inquiry*, WASH. POST (Oct. 30, 2009), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/10/29/AR2009102904597.html.
[258] *Id*.
[259] *Id*. In a subsequent *Washington Post* online question and answer forum, the Post further described that the Ethics Committee document was brought to its attention by "a source familiar with those kinds of [peer-to-peer] networks." Washington Post Q&A with Carol Leonning 1 (Oct. 30, 2009), *available at* http://www.washingtonpost.com/wp-dyn/content/liveonline/discuss/transcript_politics131.htm (last visited Sept. 4, 2014).
[260] Nakashima.
[261] *Id*.
[262] *Id*.
[263] Chairwoman Lofgren stated, "I regret to report that there was a cyberhacking incident of a confidential document of the committee. A number of Members have been contacted by The Washington Post, which is in possession of a document. We don't know with certainty whether it is an accurate document, but we thought it important to state the relevance of the material." Statement of Congresswoman Zoe Lofgren, Cong. Record, Announcement by the Chairwoman of the Comm. on Standards of Official Conduct (Oct. 29, 2009).
[264] E-mail from Rick Wallace, Analyst, Tiversa, to Robert Boback, CEO, Tiversa (Oct. 20, 2009 12:34 a.m.) [TIVERSA-OGR-0026603 - 26604].
[265] *Id*.
[266] E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock, Todd Davis, CEO, LifeLock, and Clarrisa Cerda, Counsel, LifeLock (Oct. 26, 2009 7:37 a.m.) [LLOCK-OGR-0002009].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, October 26, 2009 7:37 AM
To: Mike Prusinski; Todd Davis; Clarissa Cerda
Subject: RE: 60 minutes

"…there was a breach in House Ethics via 2P2 that the Washington Post will be writing a story about this week or next…"

As soon as I get the OK from the FBI, we will be off an running. We h[illegible] huge rings that we are tracking right now but I can't discuss as they are open investi[illegible]. We hired a new guy that came from the Secret Service to help us address these cr[illegible]s.

Also, there was a breach in House Ethics via P2P that the Washington Post will be writing a story about this week or next. Should be interesting...

Boback did not explain to LifeLock how he had become aware of the breach, or of the upcoming, and then-unpublished, *Washington Post* story.

While it is suspicious that Boback knew of the *Washington Post* story days before its publication, this Committee's investigation did not examine whether Boback or Tiversa acted as the initial source in providing the Ethics Committee document to the *Washington Post*. Documents produced by Tiversa showed that Boback provided information about the leak to the *Washington Post* reporter. On October 30, 2009, at 4:49 p.m., a *Washington Post* reporter e-mailed Boback asking whether a certain statement, including a quote from Boback, was accurate:[267]

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 4:49 PM
To: Robert Boback <rboback@tiversa.com>
Subject: RE: this accurate?

A confidential House Ethics Committee file that disclosed the status of dozens of investigations of lawmakers on issues ranging from influence lobbying to defense peddling is still available on public file-sharing computer networks, according to a security firm that specializes in scouring such networks for clients.
The document, a committee report from late July, has been downloaded by a handful of users in Washington DC, Houston, New York, Los Angeles, Toronto and London, said Robert Boback, chief executive of Tiversa Inc., the firm that was able to confirm the document was still on the networks yesterday and has technology capable of allowing it to see what tens of millions of computer users are searching for or downloading in real time on these publicly accessible networks.
The file was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had on it popular "peer-to-peer" software used for downloading free music and movies through file-sharing networks, Congressional sources said. The staffer could not be reached for comment. Her father said her attorney had advised that she not speak about the case.
The peer-to-peer premise is simple, and potentially risky. Anyone who has the software makes contents of their computer available to anyone else with the software on their computer through a "peer to peer" exchange bypassing the Web, as long as they are on a file-sharing network at the same time.
The staffer, who was the Committee's Web administrator and developed electronic spreadsheets and documents, was fired earlier this week, the sources said.

.....

Tiversa did not produce to the Committee any response Boback may have written. This is the earliest document produced to this Committee indicating that the document had "spread," i.e., that other peer-to-peer users had downloaded it. The *Washington Post* does not appear to have used Boback's quote or the information about the spread of the document in stories about the leak.

[267] E-mail from Ellen Nakashima, Wash. Post, to Robert Boback, CEO, Tiversa (Oct. 30, 2009 4:49 p.m.) [TIVERSA-OGR-0026594].

The reporter then e-mailed Boback regarding the origin of the leak. The first sentence reiterated the known information about the leaker, and the second sentence outlined generally how peer-to-peer networks operate:

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 7:47 PM
To: Robert Boback <rboback@tiversa.com>
Subject: RE: this accurate?

In the breach, the report was disclosed inadvertently by a junior staffer on the ethics committee, who apparently had stored the file on a home computer that had so-called "peer-to-peer" software, congressional sources said. The popular software, which is easily available online, allows computer users to share music or other files. But it also allows anyone with the software on their computer to access documents of another user without permission, as long as the users are on a file-sharing network at the same time.

Ellen Nakashima
The Washington Post
202 334 4419 direct
202 286 0552 cell

http://projects.washingtonpost.com/staff/articles/ellen+nakashima/

Again, Tiversa did not produce any response from Boback. The e-mail does further illustrate, though, that the reporter sought advice from Boback, at the very least, during the drafting of an upcoming piece.

Several hours later, the same reporter e-mailed Boback a third time with additional information about the leak, including "the latest" on the response by House leaders:[268]

[268] E-mail from Ellen Nakashima to Robert Boback (Oct. 30, 2009 8:08 p.m.) [TIVERSA-OGR-0026592].

From: Ellen Nakashima <nakashimae@washpost.com>
Sent: Friday, October 30, 2009 8:08 PM
To: Robert Boback <rboback@tiversa.com>
Subject: amended

File sharing networks are made up of hundreds of millions of users who periodically log on and off, with 25 million or so being active at any given moment. The typical user, when searching for files, will reach only a small portion of the users on the network--from 30 to 3,000 people, depending on the connection strength.
A search on the word "meeting" may result in anything from a PTA meeting to an Iraqi operations meeting involving sensitive military details.

Here's the latest :
House leaders on Friday called for an "immediate and comprehensive assessment" of congressional cybersecurity policies, a day after an embarrassing data breach that led to the disclosure of details of confidential ethics investigations.
Speaker Nancy Pelosi (D-Calif.) and Minority Leader John A. Boehner (R-Ohio) said they had asked the chief administrative officer of the House to report back to them on the policies and procedures for handling sensitive data as a result of the breach. The breach led to the inadvertent dislosure of a House Ethics Committee document that summarized the status of investigations into lawmakers' activities on subjects ranging from influence peddling to defense lobbying.
"We are working diligently to provide the highest level of data security for the House in order to ensure that the operations of House offices are secure from unauthorized access," Pelosi and Boehner said in a statement.
The breach angered lawmakers who were the subject of previously undisclosed investigations and raised questions about the security of other senstive documents.
Rep. Gary Miller (R-Calif.), who was named in the document as having his real estate dealings under investigation, said he was so upset about the breach that he complained Thursday evening about the matter to Rep. Zoe Lofgren (D-Calif.), chairman of the ethics committee, during a series of roll-call votes.
"This is ridiculous and amateurish," he said of the breach in the committee's files.
Even as the House leadership sought answers — and the Ethics Committee moved to review its own security policies — the newly disclosed document remained available on public file-sharing computer networks, according to security experts. As of Friday, it had been downloaded by users in Washington, New York, London and elsewhere.

Ellen Nakashima
The Washington Post
202 334 4419 direct
202 286 0552 cell

http://projects.washingtonpost.com/staff/articles/ellen+nakashima/

Again, Tiversa did not produce any response to this e-mail Boback may have written. It is therefore unclear if Boback did not respond at all to these three e-mails, responded by phone, or responded in e-mails that Tiversa failed to produce. In the third e-mail, however, information on the spread and availability is no longer attributed to Tiversa. Instead, it is attributed to "security experts." It is thus not clear if Boback asked that Tiversa not be named in the story, or if the reporter amended the information to exclude Tiversa's name without prompting. Two months later, in December 2009, Boback provided the same reporter with information about a TSA document Tiversa found on the peer-to-peer network. In that instance, Boback wrote, **"[a]s always, we are not the source. :-)[.]"**[269] The reporter responded, asking **"[w]hat again is the main reason you don't want to be identified as the source – to avoid charge [*sic*] that you're doing this for commercial gain? To preserve relationship with govt [*sic*] customers?"**[270]

[269] E-mail from Robert Boback to Ellen Nakashima (Dec. 17, 2009 2:12 p.m.) [TIVERSA-OGR-0008473].
[270] E-mail from Ellen Nakashima to Robert Boback (Jan. 4, 2010 10:36 a.m.) [TIVERSA-OGR-0008473]. Even this exchange runs contrary to statements Boback made to a potential client in July 2008. At that time, Boback wrote about another Washington Post reporter, "I know that the WashPost reporter is actively scouring the file sharing networks to find any information relevant to 'DC-area businesses…especially government contractors.' For clarity, we would never provide any information or files to any reporter whether you decided to work with our firm or not, however he will probably find them on his own if he continues to search." E-mail from Robert Boback, CEO, Tiversa, to [Redacted Name], President/CEO [Redacted Company] (July 17, 2008 2:55 p.m.) (Emphasis and ellipsis in original) [TIVERSA-OGR-0019195. Given that Boback did, in fact, provide information to a reporter on at least one occasion, it is not clear if Boback lied to this customer about Tiversa's relationship with the media, or if Boback changed his mind about this policy sometime later.

Tiversa did not produce any response to this e-mail from Boback. As such, his reasoning remains unknown.

Less than a year later, in August 2011, Tiversa entered into a contract with TSA for peer-to-peer monitoring and remediation services. The potential value of the contract over five years was $1,548,000 and the scope of the project included "help[ing] the TSA avoid negative publicity and exposure through P2P file sharing networks."[271] TSA did not exercise all option years on the contract. The Committee does not know how many years of the contract passed before TSA ended its contract with Tiversa.

Tiversa received a great deal of press attention in the wake of the House Ethics leak. *Network World* reported that Tiversa had "seen the file at multiple locations including London, Toronto, Washington, Los Angeles, Texas and New York."[272] The leak also sparked additional media interest around Tiversa's previously announced peer-to-peer discoveries.[273] In one instance, a blogger reported that Tiversa discovered the document.[274] Boback insisted that Tiversa deny "discover[y]" of the exposed report to a blogger; he maintained that Tiversa only "investigated" the breach after he was made aware of its occurrence.[275] As of September 12, 2014, the article remained unedited.[276]

Whether or not Tiversa "discovered" the leak, the documents show that although Tiversa was aware of the leak, the company failed to report the leak to the House Ethics Committee, long before the *Washington Post reported* about it.

B. Tiversa "assists" the House Ethics Committee in its investigation

While Tiversa was aware of the Ethics Committee leak more than a week before it became public, Tiversa does not appear to have contacted the Ethics Committee about the leak

[271] Contract HSTS03-11-C-CIO554 (Aug. 3, 2011) [TIV-0000101-135].
[272] Jaikumar Vijayan, *Leaked House Ethics Document Spreads on the Net via P2P*, NETWORK WORLD (Oct. 30, 2009), *available at* http://www.networkworld.com/article/2252989/securityeaked-house-ethics-document-spreads-on-the/security/leaked-house-ethics-document-spreads-on-the-net-via-p2p.html (originally published in *Computerworld*) (last visited Sept. 9, 2014).
[273] J. Nicholas Hoover, *Bill Would Ban P2P Use by Federal Employees*, INFORMATIONWEEK (Nov. 18, 2009), *available at* http://www.informationweek.com/regulations/bill-would-ban-p2p-use-by-federal-employees/d/d-id/1084955 (last visited Sept. 9, 2014) ("In October, Tiversa provided the House Oversight and Government Reform committee [*sic*] with evidence that secret military documents on P2P networks had been downloaded in China and Pakistan and that personally identifiable information on U.S. soldiers was widely available.").
[274] John Pescatore, *The Security Risks of Consumerization Hit Home for US Congress*, GARNER BLOG NETWORK (Nov. 2, 2009), http://blogs.gartner.com/john_pescatore/2009/11/02/the-security-risks-of-consumerization-hit-home-for-us-congress/ (last visited Sept. 12, 2014).
[275] E-mail from Robert Boback, CEO, Tiversa, to Scott Harrer, Brand Dir., Tiversa (Nov. 11, 2009 10:54 a.m.) (In response to an article by John Pescatore that read "I live in the Washington DC area and much Beltway buzz about the Washington Post article on Tiversa's discovery of a House ethics report only available on a peer to peer music stealing file sharing network," Boback said, "Tiversa did not discover the document…. we need to let Pescatore know about that. We only investigated the breach.") [TIVERSA-OGR-0026558].
[276] Pescatore..

prior to publication of the story by the *Washington Post*. Tiversa appears to have first spoken with the House Ethics Committee on or around November 2, 2009.

On November 2, 2009, Boback provided information about the leak to the House Ethics Committee. Specifically, Boback provided a list of IP addresses at which the House Ethics Committee document had allegedly been downloaded:[277]

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 10:13 AM
To: Stoddard, Clifford
Subject: File Spread Analysis (Tiversa)
Importance: High
Sensitivity: Confidential

Mr. Stoddard,

Please see (below) the preliminary file spread analysis that Tiversa performed. Per our discussion, I have instructed our Security Ops Team to issue takedown notices for all of the cases listed. We will continue to monitor to verify that a) no other instances of spread arise and b) the takedown notices are effective in removing the file from the PCs and therefore the network. The IP address in red below is the original source of the leak.

216.45.59.122	UNITED STATES	CALIFORNIA	LOS ANGELES	OC3 NETWORKS & WEB SOLUTIONS LLC
70.240.108.51	UNITED STATES	TEXAS	HOUSTON	AT&T INTERNET SERVICES SWBELL.NET
69.119.255.103	UNITED STATES	NEW YORK	YONKERS	OPTIMUM ONLINE (CABLEVISION SYSTEMS)
72.225.253.212	UNITED STATES	NEW YORK	NEW YORK	ROAD RUNNER HOLDCO LLC
99.234.251.73	CANADA	ONTARIO	TORONTO	ROGERS CABLE INC.
81.76.50.206	UNITED KINGDOM	ENGLAND	LONDON	ENERGIS UK
69.255.116.72	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE
98.218.86.107	UNITED STATES	VIRGINIA	ALEXANDRIA	COMCAST CABLE
76.111.69.89	UNITED STATES	VIRGINIA	ARLINGTON	COMCAST CABLE
68.48.69.117	UNITED STATES	DISTRICT OF COLUMBIA	WASHINGTON	COMCAST CABLE

If you have any questions, please email or call.

Best Regards,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

The locations of the IPs—including Washington, D.C., Houston, New York, Los Angeles, Toronto, and London—were the same as those included in the e-mails from the *Washington Post* reporter to Boback several days earlier. In a later e-mail that same day, Tiversa provided additional information about when it first located the Ethics Committee document:[278]

[277] E-mail from Robert Boback, CEO, Tiversa, to Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm. (Nov. 2, 2009 10:13 a.m.) [TIVERSA-OGR-0002413].
[278] E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].

"As an answer to your question below, the search that resulted in us finding the original source file occurred in early August. It is my assumption that it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago)."

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Monday, November 02, 2009 4:44 PM
To: Stoddard, Clifford
Subject: RE: File Spread Analysis (Tiversa)
Sensitivity: Confidential

Hi Cliff,

Our systems first acquired the file in early August using the term "report." As we provide services for ID theft pro[illegible] through our partner LifeLock, we issue several general search terms for information related to consumer security such as r[illegible]dial, meeting, password, login, medical, insurance, etc. The results of these, and our other client specific search terms, are [illegible]wnloaded to our storage arrays. We have algorithms and individuals who then review the data via specific criteria (either specific co[illegible]mer names, SSNs, DOBs, etc. or specific client names like Goldman Sachs, Cigna, Capital One etc.) to determine if our clients information has been exposed. Our searches and downloads happen continuously and downloads have averaged in excess of 100,000 new files per day. As an answer to your question below, the search that resulted in us finding the original source file occured in early August. It is my assumption it was the same day in which the source of the leak saved it to her home PC. The file, although downloaded in early August, was not reviewed by anyone here at Tiversa until recently (2 weeks ago). I am not sure if I had spoken to Oversight about this specific file as we were discussing several files at that time. Our system can also download additional files (in an automated fashion) from the same source IP in an effort to provide our CFAs (Cyber Forensic Analysts) with additional insight as to the identity of the source of the disclosure. In this situation, our system downloaded two resumes from one of the IP addresses. It was due to the resume that we were able to arrive at a suspected original source.

Unfortunately, there is no way to tell exactly when the secondary IP addresses downloaded the file.

We will continue to monitor for the presence of the file on the network as others may have downloaded the file in addition to the IPs provided. Once detected, we will issue takedown notices with the corresponding ISPs.

Best Regards,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

Before Boback sent any e-mails to the House Ethics Committee on November 2, he e-mailed a LifeLock executive about the leak as an "FYI," in case LifeLock "want[ed] to piggyback anything on this[.]"[279]

[279] E-mail from Robert Boback, CEO, Tiversa, to Mike Prusinski, Vice President, Pub. Affairs, LifeLock (Nov. 2, 2009 9:50 a.m.) [LLOCK-OGR-0002036].

From: Robert Boback [rboback@tiversa.com]
Sent: Monday, November 02, 2009 9:50 AM
To: Mike Prusinski
Subject: File sharing breach in House Ethics
Attachments: 20091029183511871.pdf

Pru,

Not sure if you saw the latest file sharing breach in Congress. See attached letter that Congress released regarding the breach. Congress is now doing a complete cybersecurity review and analysis. :-)

Just an FYI for you guys....not sure if you want to piggyback anything on this for your purposes....

Best,
Bob

Robert Boback
Chief Executive Officer

Tiversa, Inc.
The P2P Intelligence Experts
144 Emeryville Drive, Suite 300
Cranberry Township, Pennsylvania 16066
| 724-940-9030 Office | 724-940-9033 Fax

"…not sure if you want to piggyback anything on this for your purposes…"

Several days later, Boback traveled to Washington, D.C. to meet with the Chair and Ranking Member of the House Ethics Committee regarding the leak.[280] During this meeting, the Ethics Committee appears to have requested a timeline from Tiversa about the leak.[281] On November 24, the Ethics Committee again requested a timeline, apparently after additional phone conversations between the Committee and Tiversa.[282] On December 3, the Ethics Committee requested yet again that Tiversa provide the timeline first requested nearly a month earlier. The Ethics Committee also asked if Tiversa's systems had picked up the file's download from Wikisecrets.org and several other websites:[283]

[280] E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Nov. 6, 2009 2:30 p.m.) [TIVERSA-OGR-0002411].
[281] E-mail from Blake Chisam, Staff Dir. & Chief Counsel, Comm. on Standards of Official Conduct, to Robert Boback, CEO, Tiversa (Nov. 24, 2009 2:43 p.m.) ("I know Cliff's been chatting with you about the timeline that the Chair and Ranking Member discussed with you at our meeting … I can't recall seeing a timeline. Is there any chance you could shoot that over to me?") [TIVERSA-OGR-0002409]. Tiversa has not produced any documents to this Committee indicating that it replied to this request for information.
[282] *Id*.
[283] E-mail from Clifford Stoddard, Counsel, Comm. on Standards of Official Conduct, H. Ethics Comm., to Robert Boback, CEO, Tiversa (Dec. 3, 2009 7:20 a.m.) [TIVERSA-OGR-0002407].

On Dec 3, 2009, at 7:20 AM, "Stoddard, Clifford" <Clifford.Stoddard@mail.house.gov> wrote:

Bob,

Sorry to pester you but in turn I am being asked continually about the time-line issue. I understand that Tiversa system discovered the document on August 4. The global search was done on October 30. Between then, you notified the Oversight Committee, specifically, Steven Rangel. Did you find out the specific date you notified Rangel? Also, as you probably know, the document has now been made available by Wikisecrets.org and can be downloaded from several websites. Did your system pick up these new addresses?

Also, could you have someone send us the hash for the file? Thanks.

The Members will be meeting with us in an hour and will ask again for the timeline I am sure.

Regards,

Cliff

Clifford C. Stoddard, Jr.

Counsel

Committee on Standards of Official Conduct

U. S. House of Representatives

HT-2, the Capitol

Washington DC 20515

(202) 226-8810 (direct)

Boback finally responded, with a very general timeline of events:[284]

From: Robert Boback [mailto:rboback@tiversa.com]
Sent: Thursday, December 03, 2009 10:32 AM
To: Stoddard, Clifford
Subject: Re: information

Hi Cliff
I am in LA training with FBI LEEDA right now but I wanted to drop you a note in advance of your meeting. Our systems located the file on Aug 1 not Aug 4. We did perform a global scan on Oct 30. I spoke to Steven Rangel between those dates but I don't have any record of it to provide clarity as to when. During that period I probably had 15 or so conversations with him regarding other breaches. To the best of my recollection, I think that I spoke to him about the document around the week of 19th of Oct, altough it may have been sooner. We only discussed it once. Beyond that, I don't specifically recall anything. It didn't seem that sensitive to me.

Best
Bob

Sent from my iPhone

Boback did not address the Ethics Committee's concern that the file had been made available by wikisecrets.org and several other websites. Boback also provided information that contradicted his November 2, 2009, e-mail. On November 2, Boback wrote that he "was not sure if [he] had spoken to Oversight about this specific file as we were discussing several files at that time."[285] On December 3, 2009, however, Boback wrote that he spoke with an Oversight Committee staffer sometime between August 1 and October 30, likely around October 19.[286]

[284] E-mail from Robert Boback to Clifford Stoddard (Dec. 3, 2009 10:32 a.m.) [hereinafter Boback-Stoddard Dec. 3 E-mail] [TIVERSA-OGR-0002407].
[285] E-mail from Robert Boback to Clifford Stoddard (Nov. 2, 2009 4:44 p.m.) [TIVERSA-OGR-0002412].
[286] Boback-Stoddard Dec. 3 E-mail..

Boback further explained that he "probably had 15 or so conversations" with the Oversight staffer about other breaches between August 1 and October 30, and that he only discussed the Ethics file with the Oversight staffer on one occasion. Boback explained that the file "didn't seem that sensitive" to him.[287]

Further, Boback indicated in the November 2 e-mail that Tiversa reviewed the House Ethics document "about two weeks ago," meaning that Tiversa became aware of the House Ethics file in mid-October. This timeline fits with an October 19 conversation with the Oversight staffer, and the October 20 internal Tiversa e-mail in which Boback received information about a House Ethics staffer.

Tiversa, by its own admission, learned of the House Ethics document in mid-October. Boback had a conversation about the document with the House Oversight Committee, mentioned the leak to executives at LifeLock, and conducted an investigation into the source of the leak, all before publication of the story. Yet Tiversa does not appear to have contacted the House Ethics Committee about the leak prior to publication of the *Washington Post* story. Boback further appears to have provided information about the spread of the leak to the *Washington Post* days before he provided the same information to the Ethics Committee.

Had Tiversa notified the Ethics Committee about the leak in a timely fashion, then it could have prevented some or all of the alleged spread of the document over the peer-to-peer network. When presented with a chance to minimize harm to the House of Representatives, Boback failed to act. Instead, Boback's failure to inform the House Ethics Committee of the leak quickly and his failure to provide timely and consistent information about the exposed document are indicative of Tiversa's questionable business practices in general. Finally, Tiversa stood to benefit from the *Washington Post*'s publication of the House Ethics leak regardless of whether Tiversa was the initial source of the article, or whether the article cited Tiversa. Any news on the vulnerability of sensitive information to leaks breached via peer-to-peer networks—and especially a high-profile breach—would bolster Tiversa's profile as a firm with the capability to remediate this type of problem. The House Ethics leak is another example of Tiversa's use of its association with Congress as a platform for intimidation and fearmongering.

A whistleblower's account of the story states that in the course browsing the P2P network for profitable material, Tiversa came across the Ethics Committee document. Tiversa's plan, according to the whistleblower was to leak the document to the press and generate publicity for it and then sell its services to the U.S. congress as the solution to the problem while never acknowledging it was the source of the breach. This resulted needlessly in the embarrassment of many Members of Congress who did not receive investigatory due process as a result of the pending investigations being exposed.

VII. *Open Door Clinic*

[287] *Id*.

The Open Door Clinic is a small non-profit healthcare organization located in Elgin, Illinois.[288] Open Door provides education, testing, and treatment for sexually transmitted infections, including HIV/AIDS.[289] Between 2008 and 2009, Tiversa sought to exploit the Open Door Clinic using information Tiversa discovered on a peer-to-peer network.

A. Initial contact with Tiversa

On June 5, 2008, a computer with the IP address of 75.58.87.97 disclosed six files related to the Open Door Clinic on a peer-to-peer network.[290] According to information provided by Tiversa, through the Privacy Institute, to the FTC, Tiversa appears to have downloaded these six files from that IP address on or around June 5, 2008.[291] The documents—spreadsheets of patient information—exposed the names, addresses, telephone numbers, social security numbers, and HIV/AIDS status of approximately 250 Open Door patients.[292] The fact that patient information was leaked on a peer-to-peer network is not disputed, nor is the seriousness of the leak in question. The documents contain no information identifying them as the property of the Open Door Clinic— the clinic's name does not appear on any or the six spreadsheets, nor does its address, phone number, location, or any identifying information appear.[293] Tiversa has not provided information to the Committee about how it determined that these documents belonged to the Open Door Clinic.

On July 14, 2008, a Tiversa sales representative contacted the Open Door Clinic about the leak.[294] Tiversa subsequently provided one of the six documents it downloaded to the Open Door Clinic via e-mail.[295] In the e-mail, which included the password to open the document, the

---

[288] *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 113th Cong. 25 (July 24, 2014) (testimony of David Roesler, Exec. Dir. of Open Door Clinic) [hereinafter Roesler Testimony].
[289] Open Door Clinic, *History*, *available at* http://www.opendoorclinic.org/about-us/history/ (last visited Sept. 4, 2014).
[290] Microsoft Excel spreadsheet from Tiversa to FTC, "FTC Final 8-14-09pm.xls" [FTC_PROD0000014].
[291] *Id*. The exact date of download of all six documents is not fully clear to the Committee. The spreadsheet of companies created by Tiversa for the FTC indicates that the "date of disclosure" of the six Open Door Clinic files was June 5, 2008. *Id*. Tiversa informed the Committee, however, that it downloaded one of the files, "Master List.xls," on May 26, 2008 at 7:29 p.m. Letter from Reginald J. Brown, Counsel for Tiversa, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 28, 2014). Tiversa declined to provide the exact dates it downloaded the additional five files related to the Open Door Clinic "because Tiversa, Inc. believes it only analyzed the origins of the MASTER LIST.xls file." *Id*. It is not clear how Tiversa determined the date of disclosure of the six files provided to the FTC to be June 5, 2008, and why Tiversa did not inform the FTC that at least one of the files provided was downloaded the previous month. It is also not clear how Tiversa provided a "date of disclosure" to the FTC for all six documents if it in fact only analyzed one of the files.
[292] Microsoft Excel spreadsheet from Tiversa to FTC, "Master List.xls" [FTC_PROD0005345].
[293] Microsoft Excel spreadsheets from Tiversa to FTC, "Master List January 15, 2003.xls" [FTC_PROD0005340]; "Master List Michelle.xls" [FTC_PROD0005341]; "Master List Rosa.xls" [FTC_PROD0005342]; "Master List Sally.xls" [FTC_PROD0005343]; "Master List Sharon.xls" [FTC_PROD0005344]; "Master List.xls" [FTC_PROD0005345].
[294] E-mail from Perry Maier, Assistant Dir., Open Door, to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 10:56 a.m.).
[295] E-mail from Keith Tagliaferri, Cyber Forensic Analyst, Tiversa, to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 3:20 p.m.).

sales representative attached a statement of work for the Open Door Clinic to hire Tiversa.[296] The quoted rate for Tiversa's services was $475 per hour – far beyond the clinic's modest budget.[297] Open Door employees were immediately suspicious as to why Tiversa contacted the clinic:[298]

Perry Maier

From:	Perry Maier [perrym@opendoorclinic.org]
Sent:	**Monday, July 14, 2008 2:15 PM**
To:	Anders Riedemann
Subject:	Phone call
Importance:	High

"It could be an elaborate scheme to get business."

Anders: I hope that you will have a chance to speak with Katey. It could be an elaborate scheme to get business. Keep me posted. I believe she gave you her cell phone number. Perry

The Open Door Clinic began an internal investigation of the leak after receiving notification from Tiversa. In early September 2008, an IT vendor for the clinic contacted Tiversa by telephone to obtain more information about the leak and what steps the clinic could take to remediate the breach.[299] Tiversa provided eight steps that Open Door could undertake to remediate the leak:[300]

[296] E-mail from Katy Everett to Anders Riedemann, IT Adm'r, Adnet (July 14, 2008 3:29 p.m.) [Open Door e-mail #5].
[297] Roesler Testimony, at 25.
[298] E-mail from Perry Maier to Anders Riedemann (July 14, 2008 2:15 p.m.).
[299] E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 4, 2008 1:34 p.m.).
[300] *Id*.

Tuesday, January 26, 2010 1:26 PM

bject: P2P Disclosure Information
ate: Thursday, September 4, 2008 1:34 PM
From: Katy Everett <keverett@tiversa.com>
To: TJ Vinz <tvinz@adnet.us>

Hi TJ. Thank you for taking the time to speak with me on the phone this afternoon. What follows is some information you can share with the folks at Open Door in terms of recommendations we would make or best practices we have seen others follow when facing similar circumstances regarding a potential breach. First, please know that though this type of incident is not a new problem, the exposure of it as an issue is new. Extremely large companies with very sophisticated IT systems have been victim to sensitive and costly P2P disclosures (such as Pfizer, ABN AMRO, Walter Reed Army Medical Hospital, etc.) and few if any organizations are immune to its risk.

When a disclosure like this occurs, companies often go through the following steps:

1. Identify the offending computer/source (it may or may not be the computer that you have identified)
2. Identify any additional files that might have been disclosed from the offending computer/ source (this often determines/confirms the original source because often additional files are disclosed that allow us to profile the individual disclosing them)
3. Remediate/close down the offending computer/source
4. Identify any additional sources that may have acquired the file(s) and are re-sharing it/ them to the P2P networks
5. Remediate/close down any additional sources found in step #4
6. Take any notification steps required by state/industry regulatory bodies based on the severity of the information disclosed (e.g. social security numbers, etc.)
7. Provide services (e.g. credit monitoring, fraud alerts, etc.) to affected individuals
8. Document all steps taken to address both this incident and to prevent others from occurring as required by state/regulatory bodies, customers, other stakeholders, etc., and in support of any future legal defense actions

As I said earlier, Tiversa can assist Open Door with any of the above and in performing the global spread analysis we discussed. This helps many organizations inform their security breach notification proceedings as it will tell you how far the file has spread and how many pcs currently have downloaded it. As we discussed, even though the file itself may appear old, social security numbers never expire and criminals hunt for them every day on these networks in an effort to commit identity theft or fraud against individuals.

Tiversa also offered to "assist Open Door with any of the above and in performing the global spread analysis we discussed."[301] The sales representative again attached a statement of work for an Incident Response Investigation for Open Door. The quoted rate remained $475 per hour.[302]

One hour later, the Open Door Clinic's IT vendor sent these eight steps to the clinic, as well as information on how the clinic had already addressed each step in the course of its internal investigation.[303] The clinic's internal investigation, based on the limited information provided by

[301] *Id*.
[302] *Id*.
[303] E-mail from TJ Vinz, Adnet to Ryan Howater, Adnet (Sept. 4, 2008 2:40 p.m.).

Tiversa, found that none of the computers on the system had peer-to-peer software installed, and that no peer-to-peer network ports into or out of the clinic's computer system were allowed.[304] As Executive Director David Roesler testified, the clinic was at a loss as to how the one file Tiversa provided could have been exposed on a peer-to-peer network.[305]

Later that month, Tiversa again contacted the Open Door Clinic, this time attempting to sell LifeLock's identity theft services.[306] A Tiversa sales representative wrote, "Tiversa has recently established an exciting new partnership with a company called LifeLock. LifeLock is a leading provider of identity theft PREVENTION [*sic*] services to many organizations and corporations."[307]

Ultimately, Open Door declined to purchase Tiversa and LifeLock's services. In his testimony before the Committee, Roesler explained that the clinic did not purchase Tiversa's services because Open Door's IT provider had sufficiently "reviewed its network to confirm that there was no evidence of any P2P software."[308]

B. Tiversa only provided self-serving information to the Open Door Clinic in July 2008

Tiversa has maintained to the Committee that it went above and beyond in trying to help the Open Door Clinic mitigate the peer-to-peer leak. Such a statement, however, is not only self-serving, but also incorrect. In fact, Tiversa failed to provide full and complete information about the leak to the clinic.

Several of the eight steps for mitigation Tiversa suggested to the clinic—including the suggestions to "identify any additional sources that may have acquired the file(s) and are re-sharing them to the P2P networks" and "remediate/close down any additional sources found in step #4"—are steps that seemingly require the use of Tiversa's technology. Tiversa has maintained that it provides technology and services that no other company can provide. The so-called "steps" Tiversa provided are in fact a blatant sales pitch. Tiversa failed to provide additional files downloaded from the Open Door Clinic on the same day from the same IP address. Tiversa also failed to provide the IP address of the computer leaking the files, information that Tiversa's technology can provide in minutes. Had Tiversa chosen to provide the Open Door Clinic with this information, the clinic could have more readily identified the source of the leak.

Further, Tiversa appears to have begun investigating the source of the Open Door leak even prior to July 14, 2008, when it first contacted the Open Door Clinic. On July 3, 2008, Chris

---

[304] *Id*.
[305] Roesler Testimony, at 25.
[306] E-mail from Katy Everett, Tiversa, to TJ Vinz, Adnet (Sept. 24, 2008 2:20 p.m.). This e-mail was not produced to the Committee by Tiversa.
[307] *Id*.
[308] Roesler Testimony, at 25, 60.

Gormley, Tiversa's former Chief Operations Officer, e-mailed a sales representative a web link, with the notation "Open Door Clinic:"[309]

Molly Trunzo

From: Chris Gormley
Sent: Thursday, July 03, 2008 11:26 AM
To: Katy Everett
Cc: Chris Gormley
Subject: Info

http://www.effectiveinterventions.org/go/interventions/sista

Open Door Clinic

Tiversa did not produce this e-mail to the Committee. A forensic report Tiversa created in October 2011, which Tiversa also did not produce to the Committee, includes several files about the "SISTA Project" to support its conclusion that the probable disclosure source was a specific Open Door employee.[310]

The July 3, 2008, e-mail indicates that Tiversa had already begun work on step one of the eight steps provided to the Open Door Clinic—"identify the offending computer/source"—but failed to inform Open Door of this information. Further, the same sales representative who sent the eight steps to the Open Door Clinic also received Gormley's e-mail.

Had Tiversa really wanted to help this non-profit clinic, it could have provided all of the files downloaded from Open Door and the IP address of the computer sharing the files in question. Tiversa could have also informed the clinic that it had already begun investigating the source of the breach, and had identified a potential link between documents the computer shared and the identity of the computer's owner.

C. Tiversa facilitates a class action lawsuit against the Open Door Clinic, and contacts Open Door patients directly

On July 29, 2009, Tiversa CEO Robert Boback testified about the Open Door Clinic leak before the Committee. Boback stated that 184 Open Door patients were "now victims of identity

[309] E-mail from Chris Gormley, COO, Tiversa, to Katy Everett, Tiversa (July 3, 2008, 11:26 a.m.) [hereinafter July 3 Tiversa E-mail].
[310] Tiversa, *Forensic Investigation Report: Open Door Clinic*, at 6, 21, 26, 29 (Oct. 13, 2011). One of the excerpted documents in the Investigative Report discusses the SISTA Training Institute, and refers participants to the website www.effectiveinterventions.org – the same main website as the link in Gormley's July 3, 2008 e-mail (July 3 Tiversa E-mail).

theft."[311] After this hearing, a Committee staffer expressed concern to Boback that the affected Open Door clients had not been notified that their personal information had been exposed.[312]

Rather than contacting the Open Door Clinic to provide additional information about the leak that Tiversa initially withheld, such as the IP address of the source computer, the additional files that Tiversa downloaded, or any investigation Tiversa performed into the identity of the disclosing source, Boback provided information on the Open Door leak to Michael Bruzzese, one of Tiversa's attorneys.[313] Shortly after the July 2009 hearing, Boback provided Bruzzese with a verbal summary of what he knew about the Open Door leak.[314] Boback also provided one of the six documents Tiversa downloaded from the clinic.[315] At this time, Boback stated that Tiversa had also determined that an "information aggregator" located in Apache Junction, Arizona downloaded Open Door's documents.[316] Boback did not provide Bruzzese with information about any other spread at this time.[317] Boback also did not provide the Open Door Clinic with information about the alleged spread of the file.

Bruzzese and his co-counsel "retained the services of an attorney who devotes his practice to matters involving legal ethics and the rules of professional responsibility to provide us legal advice as to how and in what manner we could solicit potential clients for this case."[318] Bruzzese determined that "it was permitted to contact the potential class members by mail" and sent letters to all patients on the list Boback provided.[319] The letter was a "solicitation to provide legal services," and asked the recipient to sign on as a class representative for the suit.[320]

Tiversa, through one of its current attorneys, explained to the Committee why Tiversa provided information to Bruzzese instead of contacting Open Door or its patients directly. The attorney stated that Tiversa did not have the resources to contact the patients itself, and accordingly provided the information to an attorney:

---

[311] *Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 12 (July 29, 2009) (testimony of Robert Boback, CEO of Tiversa, Inc.). Michael Bruzzese, however, told the Committee that he did not know what would have been the basis of this statement; he was not aware of any claims of identity theft until after he assembled plaintiffs for the class action lawsuit between November 2009 and February 2010. H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Michael Bruzzese, at 115 (Sept. 10, 2014) [hereinafter Bruzzese Tr.].
[312] Letter from Michael J. Bruzzese, Att'y, Johnson, Bruzzese & Temple, LLC, to Hon. Darrell E. Issa, Chairman, H. Comm. on Oversight & Gov't Reform 2 (July 30, 2014) [hereinafter July 30 Bruzzese Letter].
[313] *Id.*
[314] Bruzzese Tr. at 21-22.
[315] *Id.* at 22.
[316] *Id.* at 32. A draft version of the Tiversa Forensic Investigation Report includes a file spread analysis. This analysis indicates that the file spread to four IP addresses unrelated to the initial disclosing source. The spread analysis shows that, in addition to the Apache Junction user, a peer-to-peer user in the Netherlands had also downloaded at least one of the Open Door files on March 12, 2009. It is not clear how Boback knew about the spread of the file in one instance, but not the other. Tiversa, *Forensic Investigation Report: Open Door Clinic* (Oct. 21, 2011) (draft report). At no point was Tiversa's file spread analysis provided to the Open Door Clinic.
[317] Bruzzese Tr. at 32-33.
[318] July 30 Bruzzese Letter at 2.
[319] *Id.*; *see also* Letter from Michael Bruzzese & James Cirilano, Cirilano & Associates, to [Open Door Clinic Patient] (Nov. 4, 2009) [hereinafter Bruzzese Patient Letter].
[320] Bruzzese Patient Letter..

> Here's what our understanding is. And, again, I think you're going to get a letter. . . . Tiversa found the Open Door file. They called them, as is their policy, just saying, look, we found this on your system, here it is. They said, no, thanks, about getting help.
>
> Getting ready for the testimony in 2009, they told the story to someone on staff. And when they told them the story, they were told back that somebody needs to reach out to the victims.
>
> **Tiversa did not have the resources to do it themselves, and they just gave a file to the local Pittsburgh attorney**, who they knew, in order to help the victims. And Tiversa didn't get any payment for it.[321]

He further stated:

> Well, what he did with it, I don't think -- Tiversa didn't say, go do this or that. It was, they were asked by staff to make sure the victims knew that their information was compromised. **And since they didn't have the ability to do it themselves, or more than what they did, they gave the information to this guy, and he said he would handle it.**[322]

Bruzzese also explained to the Committee how he contacted the clients of the Open Door Clinic. He stated:

> Q. How did you contact [the Open Door clients]?
>
> A. We contacted them one way, the only way, by sending them what in our profession is called an attorney solicitation letter, and prior to doing that, I retained the services of a lawyer in Pittsburgh who kind of concentrates his area of practice on professional responsibility and ethics and asked him whether and how under Illinois law that I could contact these individuals. And he did some research, told me **that I was prohibited from making direct phone calls to them but that I could send a letter as long as I marked on the letter that it was a solicitation from a lawyer.** And that's what we did.
>
> * * *
>
> A. Correct. So let me just make a statement to you. **Prior to the five individuals retaining my services as their lawyer, I did not make any telephone calls to any Open Door Clinic patients.**

[321] Hopkins Tr.at 143-44.
[322] *Id*. at 145 (emphasis added).

Q. Did you ask Mr. Boback if Tiversa could make telephone calls to any of the Open Door patients?

A. No.

Q. **Did you ask Mr. Boback to contact the Open Door patients in any way?**

A. **No.** [323]

Documents obtained by the Committee, however, show that Tiversa independently contacted patients of the Open Door Clinic about the leak.[324]

As these documents call into question information provided by Tiversa to the Committee, the Committee obtained phone records showing long-distance calls from Tiversa's office during the time in question. **A comparison of the phone records to documents Tiversa downloaded from the Open Door Clinic, which contained patients' personal information, clearly shows that Tiversa called more than 50 patients of the Open Door Clinic between October 29 and November 5, 2009.** Tiversa called at least one patient on multiple occasions. These phone calls from Tiversa took place just days before Bruzzese sent a letter to Open Door patients.

It is not clear why Tiversa provided false information to the Committee about whether the company contacted any Open Door patients. Further, it is not clear why Tiversa lacked the resources to contact Open Door patients, as the company represented to the Committee through its attorney. In fact, Tiversa did contact over 50 patients of the clinic. It is also not clear why Tiversa would contact over 50 patients of the clinic in late October and early November 2009, days before Bruzzese sent a letter to patients of the clinic, and following the Committee staffer's July 2009 alleged notification that patients needed to be notified.

In September 2009, Tiversa again contacted Open Door to report that the breached document was still exposed on the peer-to-peer network.[325] Again, Open Door performed its own investigation of its servers and again found no evidence of any peer-to-peer networks.[326] Tiversa did not tell Open Door that it had referred information about the leak to an attorney, nor did Tiversa provide any of the information previously withheld from the clinic. Although Tiversa professed it was concerned about notifying the patients of Open Door about the leak of personally identifiable information, it still omitted key information.

Six patients agreed to join the class action against the Open Door Clinic, and Bruzzese filed the lawsuit in February 2010. During discovery, Open Door subpoenaed Tiversa and

---

[323] Bruzzese Tr. at 35-36 (emphasis added).
[324] *See, e.g.* e-mail from Barb Cox to David Roesler, Dir., Open Door Clinic (Nov. 5 2009 4:29 p.m.) ("According to [redacted]-triversa [*sic*] called him first and asked a ton of questions-did they know that open door had done this etc. I think that Triversa [*sic*] is affiliated with the law firm and sent them the info they had-I would imagine that they get a finders fee [*sic*].").
[325] Roesler Testimony, at 25.
[326] *Id.* at 25-26.

finally received the additional files that Tiversa downloaded from the same computer on the same day as the one file it previously provided.[327] This production included information indicating that an IP address in Apache Junction, Arizona, downloaded all six Open Door files.[328] Bruzzese testified to the Committee that he also did not receive a full accounting of all the Open Door files Tiversa downloaded until he received Tiversa's production.[329]

After receiving full information from Tiversa, the Open Door Clinic determined that the source of the breach was a computer stolen from the clinic in 2007.[330] Open Door believes that the peer-to-peer software that exposed its patients' personally identifiable information was installed on the computer after it was stolen, and therefore was not a breach of Open Door's network.[331]

D. Tiversa did not charge Bruzzese for the same information it refused to provide to the Open Door Clinic

Tiversa did not accept payment for any services provided as part of the litigation against the Open Door Clinic.[332] When Boback first told Bruzzese about the Open Door leak, Boback was "adamant"[333] that Tiversa would provide any required services free of charge:

> He said, Tiversa does not want anything. I do not want anything. I am doing this to—words to this effect—discharge my obligation put upon me by the staffer to do something about it. **And he said that, whatever you need, in terms of forensic work, you've got, no matter what.**[334]

Pursuant to this professed sense of moral obligation, Tiversa performed forensic analysis of the Open Door Leak. Tiversa examined the source of the leak, including details about the 27 times the IP address shifted, the identity of the leak, and the alleged spread of the leak. Tiversa produced a 42-page forensic investigation draft report,[335] and a 39-page final forensic investigation report[336] for Bruzzese's use in the litigation.

Boback directed that Tiversa expend time and effort to investigate the leak for Bruzzese at no charge. He provided the exact same services to Bruzzese for free that he withheld from the Open Door Clinic. Had Boback really felt a sense of moral obligation to the patients of the Open

---

[327] *Id*. at 94.
[328] The production included a spreadsheet titled "Open Door Clinic File Listing With Spread" and included a list of files for two IP addresses. One IP address is the disclosing source as identified by Tiversa, and the other IP address at the time resolved to Apache Junction, Arizona. Tiversa Production to Open Door Clinic (Jan. 21, 2011).
[329] Bruzzese Tr. at 34.
[330] Roesler Testimony, at 91.
[331] *Id*. at 93.
[332] Bruzzese Tr. at 65-66.
[333] *Id*. at 65.
[334] *Id*.
[335] Tiversa, *Forensic Investigation Report* (Oct. 13, 2011.
[336] Tiversa, *Forensic Investigation Report* (Oct. 21, 2011)..

Door Clinic, he could have provided these services to the Open Door Clinic. Once again, Tiversa was in a position to help and refused to do so.

According to a whistleblower, Tiversa engaged in numerous attempts to get the Open Door Clinic to pay for its services. When the clinic refused, Tiversa began calling the patients listed on the document it downloaded. Tiversa employees thought that by calling the patients and ginning up the leak, they could scare the clinic into hiring Tiversa. When this plan failed, Boback provided the information to his attorney, Michael Bruzzese, who filed a law suit against the non-profit clinic while TIversa performed work related to the exposure free of charge to Bruzzese. The clinic was never informed by Bruzzese that Bruzzese received the information from Tiversa.

E. Tiversa provided information on the Open Door Clinic to the FTC

In addition to providing information to assist Bruzzese in his class action lawsuit, Tiversa also provided information on the Open Door Clinic leak to the FTC. Tiversa, through the Privacy Institute, provided all six documents about the clinic to the FTC. As noted above, the spreadsheet Tiversa provided indicated that all six documents were downloaded from the same IP address and disclosed on the same day – June 5, 2008.[337] On January 19, 2010, the FTC sent a letter to Open Door Clinic about the leak.[338] The letter informed the clinic that a file had been exposed on the peer-to-peer network, and noted that the clinic's failure to prevent the document from leaking could violate federal laws.[339]

If Boback was truly motivated to help the patients affected by the Open Door leak, he should have given complete information to Open Door immediately. Instead, Boback withheld critical information about the number of downloaded documents, the IP address of the leak, and any information Tiversa had uncovered about the source of the leak. He referred the leak to an attorney. Even after the referral, Tiversa made unsolicited calls to more than 50 patients of the clinic about the leak for unknown reasons. And, finally, Boback provided the very information and services he denied to the Open Door Clinic for free to the attorney who sued the Open Door Clinic over the leak Tiversa first identified. Boback's actions toward the Open Door Clinic unfortunately fit a pattern of self-promotion and manipulation, not a heartfelt wish to "discharge [his] obligation" to Open Door's clients.

VII. *Conclusion*

The Committee's investigation raises substantial questions about Tiversa's business practices. The company's failure to produce documents responsive to the subpoena hindered the Committee's investigation. Not only did Tiversa primarily report companies to the FTC that had

[337] Microsoft Excel spreadsheet from Tiversa to FTC, "FTC Final 8-14-09pm.xls" [FTC_PROD0000014].
[338] Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Protection, Federal Trade Comm'n, to Open Door Clinic (Jan. 19, 2014).
[339] *Id*.

refused its services, but it also manipulated its relationship with the FTC—including its knowledge of upcoming investigations—in an attempt to profit from these same companies the second time around. In addition, Tiversa seemingly knew about a breach at the House Ethics Committee nine days before the *Washington Post* reported about the breach. Boback notified LifeLock about the breach and the upcoming article, but failed to notify the House Ethics Committee itself. Boback's communications prior to the publication of the article call into question his claim that he did not act as the *Washington Post's* source. Finally, Boback's actions toward the Open Door Clinic are unethical, and potentially illegal. Boback refused to provide critical information about a leak of incredibly sensitive data. Instead, he reported the clinic to the FTC, provided information on the leak to an attorney, and provided certain services to the attorney free of charge but not to the clinic at all.

Boback's actions on behalf of Tiversa demonstrate that when, in a position to prevent harm to companies or the federal government, he acted to benefit himself and Tiversa. Federal departments and agencies should be aware of these business practices when determining whether to do business with Tiversa.

EXHIBIT 36

EXHIBIT 1

Sep 09 2013

Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)

Article or Commentary, Breaches

Back in July, I reported that **LabMD** had unsuccessfully attempted to sue **Tiversa** in Georgia for allegedly stealing its property. At issue was a file containing PHI on 1,178 patients that Tiversa had downloaded as part of a research project after the file was exposed via P2P software on LabMD's system. In its 2009 press release on its research, Tiversa did not name LabMD, but the matter eventually came to the FTC's attention, who opened an investigation and took LabMD to court when it failed to fully comply with an investigative demand. LabMD was ordered to comply, and in August, the FTC sued LabMD for failure to adequately protect consumer information. LabMD responded forcefully to the complaint in a press statement, alluding to Tiversa as "Internet trolls." In other statements, they've described Tiversa in other unflattering terms.

Now it seems that Tiversa is suing LabMD. Erin McAuley reports:

> A cyber-intelligence company and its CEO sued the author of the book "The Devil Inside the Beltway," claiming it falsely accused them of assisting "abusive government shakedowns" through "government-funded data mining & surveillance."
>
> Tiversa Holding Corp. and its co-founder and CEO Robert Boback sued LabMD Inc. and its CEO/author Michael J. Daugherty, in Federal Court.
>
> Daugherty's book is slated for publication on Sept. 17, by (nonparty) Broadland Press. Advance material published on the Internet identifies Daugherty as the CEO of LabMD.
>
> [...]
>
> Boback and Tiversa claim the book defames them: "In his video 'trailer' for the book, available on Mr. Daugherty's personal website, Mr. Daugherty highlights his position as LabMD's president and CEO and Mr. Daugherty alleges that Tiversa is part of a 'Government Funded Data Mining & Surveillance' scheme that engages in 'Psychological Warfare' and helps to assist in 'Abusive Government Shakedown[s].' See www.michaeljdaugherty.com. More specifically, Mr. Daugherty alleges Tiversa is conducting '300 Million Searches per day' for 'Homeland Security' and the 'Federal Trade Commission.'

Read more on Courthouse News.

Seemingly lost in most of the legal wrangling is the fact that it seems that no one whose data were in the "1718 file" were notified of the P2P exposure under HIPAA because LabMD took the position that no breach (as defined by HIPAA in 2008) had occurred.

So is HHS investigating this at all? HHS has not yet responded to an email sent by PHIprivacy.net inquiring as to whether HHS had ever opened (or concluded) an investigation of this incident. This post will be updated when I receive a reply.

Update: An HHS spokesperson responded to my inquiry with the following statement:

> OCR decided not to join FTC in their investigation of these p2p sharings and we did not independently receive complaints. As you note, this was pre-HITECH, so there was and is

Featured Articles

- NHS sells a billion patient records
- Louisiana lawmakers want to keep a state database of people who have medication-induced abortions
- Audit finds high-risk security vulnerabilities in the automated systems used to process Medicaid claims
- WA: Skagit County Government Settles Potential HIPAA Violations

Recent Posts

- Service Coordination Inc. also affected MD Department of Health and Mental Hygiene patients
- Business associate of Maryland Developmental Disabilities Administration hacked in October
- Where there's a breach, there's a lawsuit
- AZ: Hospitalists of Arizona laptop stolen from St. Mary's Hospital contained patient information
- NHS sells a billion patient records
- Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- CO: Valley View Hospital hacked; 5400 patients affected
- Meanwhile, in the LabMD case…
- UK: Home care agency warned after vulnerable people's details left in the street
- StayWell breach affects over 12,000; how many more not disclosed (update1)

Recent Comments

- Trish Harkness on Leader of Stolen Identity Refund Fraud Ring Sentenced to Jail
- Dissent on StayWell breach affects over 12,000; how many more not disclosed (update1)
- dewluca on StayWell breach affects over 12,000; how many more not disclosed (update1)

News Sections

Select Category

Archives

Select Month

RX649 PUBLIC

no obligation on LabMD with respect to our breach notification requirements — whether any exist under state law would be for the state to determine.

Posted by Dissent at 3:32 pm

Tagged with: LabMD

4 Responses to "Meanwhile, back in court: Tiversa sues LabMD for defamation, seeks to block publication of book by LabMD CEO (updated)"

1. **David Szabo** says:
September 10, 2013 at 2:22 pm

The Interim Final Breach Breach Notification Rule did not become effective until September 2009. So if the breach occurred in 2008, is its unlikely that a report was required.

> **Dissent** says:
> September 10, 2013 at 2:40 pm
>
> I suspect you're right, and I had made the same point in my July post about the incident pre-dating HITECH. But those data may now have been in a number of hands since HITECH went into effect, so what then? I would think that the PHI lost any HIPAA protection it might have had once it came into the FTC's hands, but how many parties have had access to the data since September 2009, and should HHS be looking into this?
>
> **Dissent** says:
> September 12, 2013 at 3:36 pm
>
> HHS responded to my inquiry. See the update at the bottom of the post. You were correct.

2. **Doc Sheldon** says:
September 14, 2013 at 5:37 pm

I would think that Tiversa's counsel would have advised Mr. Boback that there's little hope of winning a case claiming slander, libel or defamation, when the subject statements can be proven to be true.

It also seems a bit difficult to base a lawsuit upon statements in a book that hasn't yet been published. I guess I'm just a stickler for details.

Sorry, the comment form is closed at this time.

ICS Collection Service, Inc. press release on data breach affecting University of Chicago Physicians Group patients

Update to the inVentiv/Adheris lawsuit against HHS over prescription refill reminder programs

© 2012 PHIprivacy.net

Suffusion theme by Sayontan Sinha

EXHIBIT 37

In the Matter of:

LabMD, Inc.

May 20, 2014
Trial - Public Record
Volume 1

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION

I N D E X

IN RE LABMD, INC.

TRIAL VOLUME 1

PUBLIC RECORD

MAY 20, 2014

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
HILL	81				

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
(none)				
JX				
Number2	6			

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 20, 2014
10:11 a.m.
TRIAL VOLUME 1
PUBLIC RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
MARGARET LASSACK, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
MICHAEL PEPSON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

13

1 information of approximately 10,000 consumers, Mr. Kam
2 and Mr. Van Dyke will describe, based on their
3 experience and research, the likelihood that consumers
4 will suffer identity theft, medical identity theft and
5 other substantial harms.
6 JUDGE CHAPPELL: Do you plan to offer any
7 evidence of actual harm in this case?
8 MR. SHEER: Complaint counsel will not be
9 putting up identity theft victims, but that does not
10 mean that actual harm did not occur. And that is
11 because, in many cases, identity theft victims are
12 unable to connect up the dots. They're unable to
13 identify the source of the information that was used to
14 harm them.
15 And that's particularly the case here because
16 LabMD did not provide notice to the 9300 consumers whose
17 information was found on the P2P network. And that's
18 especially true for the hundred thousand people whose
19 information -- who did not even know that LabMD had its
20 information, their information.
21 The evidence will show that these risks are
22 particularly acute for the 9300 consumers --
23 JUDGE CHAPPELL: Hang on a second.
24 So if I understood your answer, you don't plan
25 to introduce evidence of harm, but your position is

14

1 that doesn't mean no harm occurred? Is that what you
2 said?
3 MR. SHEER: That's correct.
4 JUDGE CHAPPELL: Okay.
5 MR. SHEER: And I'm also saying, though, that
6 the legal standard is that we -- the legal standard is
7 caused harm or is likely to cause harm.
8 JUDGE CHAPPELL: I'm aware of the standard,
9 sir.
10 MR. SHEER: The evidence will show that
11 consumers cannot avoid these harms. Physicians, rather
12 than consumers, decide to use LabMD. Consumers do not
13 have information about LabMD's security practices and
14 cannot evaluate whether the practices are reasonable.
15 LabMD's security failures were not close to
16 being reasonable. As a preview, consider three obvious,
17 longstanding security issues at LabMD.
18 First, the evidence will show that LabMD failed
19 to adequately assess risks, with the result that very
20 serious, well-known and easily fixed vulnerabilities
21 went unpatched for years on the company's servers that
22 handled sensitive information.
23 For example, it did not conduct external
24 vulnerability scans to find commonly known or reasonably
25 foreseeable risks until 2010.

15

1 Second, despite it being common knowledge that
2 easily guessed passwords are a security no-no, LabMD
3 allowed employees with access to sensitive information
4 to log into their computers using, quote-unquote,
5 "LabMD" as their password. One such employee used this
6 password for years without being required to change it.
7 LabMD did not use the password management function
8 already built into the Windows operating systems it was
9 using to ensure that passwords were strong.
10 Third, IT employees and non-IT employees were
11 inadequately trained. IT employees did not receive
12 periodic security training to keep up with evolving
13 threats and how to address them. Some non-IT employees
14 could install unauthorized programs and disable security
15 settings on their computers without approval, but they
16 weren't trained that doing so could compromise the
17 security of LabMD's networks.
18 These and other security failures increased the
19 risk of unauthorized disclosure of sensitive information
20 on LabMD's network.
21 One result was that an employee installed a
22 peer-to-peer file-sharing program called LimeWire on a
23 computer used by LabMD's billing manager. LimeWire
24 allows users to designate files that they will share
25 from their own computers, search for files on other

16

1 computers and download them.
2 An insurance billing file that was designated
3 for sharing from the billing manager's computer was
4 found at IP addresses in Arizona, San Diego,
5 Costa Rica, and London. The file, which we call the
6 1718 File, contained information about more than
7 9300 consumers.
8 JUDGE CHAPPELL: Excuse me. You say this
9 information was found in these various places. How was
10 it found?
11 MR. SHEER: It was found by a third party who
12 was searching the P2P networks.
13 JUDGE CHAPPELL: And what was their motivation
14 to be searching?
15 MR. SHEER: The motivation of the search is
16 that the third party is in the business of trying to
17 protect the information of its clients, and it does so
18 by searching P2P networks, looking for information
19 about the clients. In doing that, it came across these
20 files.
21 JUDGE CHAPPELL: Is this a
22 non-government-affiliated entity?
23 MR. SHEER: It is.
24 JUDGE CHAPPELL: Not funded by taxpayer money in
25 any way?

17

1 MR. SHEER: It is not.
2 As I was saying, the file, which we call the
3 1718 File, has very sensitive information about
4 9300 consumers, including their names and
5 Social Security numbers and medical test codes. Their
6 test codes reveal the nature of the tests performed,
7 such as for prostate cancer or sexually transmitted
8 diseases or hepatitis.
9 The evidence will show that unauthorized
10 disclosure of this kind of information causes or is
11 likely to cause substantial injury in the form of
12 identity theft, medical identity theft and other harms.
13 Complaint counsel's information security expert,
14 Indiana University computer science professor
15 Raquel Hill, will explain that the 1718 File incident
16 was only the tip of LabMD's security iceberg. This case
17 is not about a single, isolated failure. It's about
18 systemic, easily addressed security failures that
19 persisted for years.
20 The evidence will show that LabMD
21 systematically failed to practice what IT practitioners
22 call defense in depth. Although it will sound
23 technical, some points, the main point is simple. LabMD
24 failed to implement the basic, simple, effective
25 security measures to protect the information in its

18

1 care.
2 So what's defense in depth on a computer
3 network? A bricks-and-mortar analogy is a castle
4 defended with a moat and sturdy inside and outside
5 walls. These multiple defenses are effective, because
6 if one defense fails, there will be another one to back
7 it up.
8 As Professor Hill will explain, defense in depth
9 on a computer network is the same concept. Use a
10 variety of security measures at the network perimeter
11 and inside the network. That way, if one measure fails,
12 other measures will protect the network.
13 Professor Hill will explain that the particular
14 security measures that accomplish reasonable defense in
15 depth for a network start with understanding the network
16 and its vulnerabilities and weaknesses.
17 JUDGE CHAPPELL: This defense in depth you're
18 talking about, is this a law, regulation or guideline
19 that's out there for everybody to see?
20 MR. SHEER: This is the practice that
21 information security professionals use and have used for
22 many, many years. It is available in many forms,
23 including in standards that have been produced by the
24 government, the National Institute of Science and
25 Technology, as well as many other private organizations

19

1 that supply information to --
2 JUDGE CHAPPELL: I'm talking about government
3 only. My question goes to the government only.
4 MR. SHEER: Yes.
5 JUDGE CHAPPELL: Law, regulation or guideline
6 published by the government.
7 MR. SHEER: There are guidelines that have been
8 published, for example, having to do with the security
9 of health information that have these same basic
10 concepts built into them. They're not always called
11 defense in depth, but there are a series of standard
12 steps, which we're going to talk about, that will
13 illustrate what "defense in depth" means.
14 JUDGE CHAPPELL: These guidelines have been
15 published. Can you cite me to them right now?
16 MR. SHEER: I can point you to the -- I can
17 point you to pieces of it right now. I can point you to
18 the HIPAA security rule which has -- which lays out in
19 some detail what defense in depth requires.
20 JUDGE CHAPPELL: Did you say HIPAA?
21 MR. SHEER: I did.
22 JUDGE CHAPPELL: Okay.
23 MR. SHEER: And I can point you, if you will
24 give me a few moments, to other sources at the
25 National Institute of Standards and Technology.

20

1 JUDGE CHAPPELL: That's fine. I don't expect
2 you to in your opening. I'm just wondering if you're
3 going to do it here in the trial.
4 Is it part of your case?
5 MR. SHEER: References have been made to those
6 things by our experts.
7 As I was saying, Professor Hill will explain
8 the particular security measures that constitute
9 reasonable defense in depth for a network start with
10 the network and its vulnerabilities and weaknesses.
11 Defense in depth counters these threats by putting in
12 place a series of roadblocks to close the
13 vulnerabilities and weaknesses at different layers of
14 the network.
15 Reasonable defense in depth is proactive, not
16 static. This is because threats and attack methods
17 change quickly, and security has to keep pace to be
18 effective. That, for example, is the point of regularly
19 updating antivirus programs.
20 At least for networks that connect to the
21 Internet, like LabMD's, defense in depth is not a
22 "set it up and forget it" endeavor.
23 Can we have slide 1, please.
24 I'd like to turn to LabMD's security failures.
25 The evidence -- the evidence will show that there were a

29

1 P2P file-sharing programs, will explain that by 2005,
2 IT practitioners were well aware of the risk that P2P
3 programs and their users would inadvertently share
4 files they did not intend to share, such as business
5 files containing sensitive information. Inadvertent
6 file sharing occurs because users mistakenly designate
7 files for sharing.
8 The evidence will show that LimeWire was
9 installed on the LabMD computer in 2006. The billing
10 manager used LimeWire to share music.
11 Also designated for sharing from the computer
12 was every file in the Windows My Documents folder, which
13 is the default folder for a user's files.
14 In all, more than 900 files were designated for
15 sharing from the computer, including, most likely
16 inadvertently, the 1718 File and other LimeWire LabMD
17 business files.
18 Would you bring up slide 6, please.
19 Slide 6 is a screen shot of LimeWire taken from
20 the computer used by LabMD's billing manager.
21 And now can we have slide 7, please.
22 Slide 7 has two highlighted lines. One shows a
23 file -- it's the lower one I believe --
24 JUDGE CHAPPELL: Is that my glasses or is that
25 blurred?

30

1 MR. SHEER: It is blurry. And I apologize for
2 that. This is the best that we can do with what we
3 received.
4 But if you look at the lower box, you will see
5 three files. One of them is being highlighted now in
6 yellow. It's called the Insurance Aging_6.05.071.pdf,
7 and it's available for sharing. This is the 1718 File's
8 true name.
9 The upper bullet or the upper box has a
10 highlighted line, and it shows that there were 950 files
11 available for sharing from this computer.
12 The evidence will show that LabMD's ordinary
13 inspections did not find the LimeWire program.
14 JUDGE CHAPPELL: Was this employee authorized to
15 use LimeWire?
16 MR. SHEER: LabMD is going to tell you no. And
17 what the evidence is going to show, however, is that
18 there were inadequate controls, as we will get to,
19 inadequate controls to prevent this employee from
20 downloading -- from installing -- downloading and
21 installing LimeWire on the computer and using it.
22 JUDGE CHAPPELL: Was that a no?
23 MR. SHEER: That was a no.
24 The evidence will show that LabMD's ordinary
25 manual inspections did not find the LimeWire program.

31

1 LabMD found it on the computer two years after the
2 program was installed and then only because it was
3 informed by a third party that the 1718 File was
4 available on a public P2P network.
5 I'm going to turn now to the next of the
6 security failures at LabMD, so we'll go back to slide 1,
7 and this is authentication.
8 The evidence will show that LabMD did not
9 require employees and others to use appropriate
10 authentication -- authentication-related security
11 measures.
12 Professor Hill will explain that LabMD did not
13 have a strong password policy and did not use measures
14 to ensure that employees use strong passwords.
15 Could you pull up slide 8 now, please.
16 Slide 8 is a 2010 table of user names and
17 passwords.
18 JUDGE CHAPPELL: Let's back up the truck here.
19 This LimeWire program you're talking about, if
20 that had never been downloaded by an employee, would we
21 not be here today?
22 MR. SHEER: It is likely that we would not know
23 about the defects in LabMD's security practices had we
24 not known that LimeWire was out on the -- that --
25 rather, that the 1718 File was on the P2P network.

32

1 JUDGE CHAPPELL: So whatever information got out
2 there in cyberspace was a result of LimeWire?
3 MR. SHEER: It was a result of the company's
4 security failures that allowed LimeWire to be used by an
5 employee to --
6 JUDGE CHAPPELL: But directly, was it a result
7 of LimeWire directly? Is that how it got on the
8 Internet?
9 MR. SHEER: Yes, it is.
10 JUDGE CHAPPELL: Thank you.
11 MR. SHEER: Going back to this exhibit, it is a
12 2010 table of user names and passwords at LabMD. It
13 shows that a number of employees were able to use or
14 allowed to use, quote-unquote, "LabMD" as their
15 password. The vertical line in yellow identifies all
16 of the instances in which that password "LabMD" was
17 used.
18 The evidence will show that reasonable
19 security -- password security practices would have
20 prevented employees from using "LabMD" or other easily
21 guessed passwords.
22 The last entry in the billing department's
23 section on this exhibit -- it's the horizontal line --
24 identifies "sbrown" as a user name and "labmd" as the
25 corresponding password.

133

1 **What are some examples of organizations that**
2 **provide such guidance?**
3 A. Some organizations that provided such guidance
4 include the National Research Council. They provided
5 an actual book, and in one chapter of the book they
6 focus specifically on security mechanisms for
7 protecting an infrastructure that contains medical
8 information.
9 **Q. What is the National Research Council?**
10 A. The National Research Council is an
11 organization that seeks the guidance of researchers in
12 the field in order to define and specify guidelines.
13 **Q. When you say "researchers in the field," what**
14 **field are you referring to?**
15 A. For this, for the purposes of this, I'm
16 referring to like IT-related individuals.
17 **Q. Are there other examples of organizations that**
18 **provide guidance for creating a comprehensive**
19 **information security program?**
20 A. The National Institute of Standards, NIST,
21 provided guidelines. I've actually cited some of their
22 guidelines on risk assessment, and so they provide a
23 comprehensive plan for risk assessment.
24 **Q. What is the full name of NIST?**
25 A. The National Institute for Standards.

134

1 **Q. What does the "T" stand for?**
2 A. I'm trying to remember what the "T" stands for.
3 **Q. Is there a document that would refresh your**
4 **memory?**
5 A. Yes, there is.
6 JUDGE CHAPPELL: Is it "Technology"?
7 BY MS. LASSACK:
8 **Q. Professor Hill, Your Honor asked if it's**
9 **"Technology."**
10 **Is it "Technology"?**
11 A. It probably is "Technology." Thank you,
12 Your Honor.
13 JUDGE CHAPPELL: And is the "S" "Science"?
14 BY MS. LASSACK:
15 **Q. Is the "S" "Science"?**
16 A. I don't recall.
17 JUDGE CHAPPELL: I'm guessing. I don't know.
18 THE WITNESS: Yeah. Actually, the "S" is
19 "Standards."
20 BY MS. LASSACK:
21 **Q. I believe you testified it's "Standards."**
22 A. Yes.
23 **Q. So then what is the full name of NIST for the**
24 **record?**
25 A. The National Institute for Standards and

135

1 Technology.
2 **Q. How would IT professionals know about**
3 **organizations like NIST and their resources?**
4 A. Organizations would know about NIST and their
5 practices and some of these other related organizations
6 through training.
7 **Q. What types of topics are covered in guidance**
8 **provided by organizations like NIST and NRC?**
9 A. The types of guidance that's provided by these
10 organizations in their guidelines are the same types of
11 guidelines that I presented in the background section
12 for a comprehensive information security program.
13 **Q. Can you remind us what those are?**
14 A. Okay.
15 So they include things like don't keep what you
16 don't need, patching your and updating your system,
17 closing all unused ports, you know, providing physical
18 security, specifying policies, you know, being able to
19 probe your network for risk assessment, those types of
20 policies, protecting your network, you know, which
21 mechanisms are best suited to address a particular
22 security goal. Those are the types of things that they
23 provide guidelines and guidance on.
24 **Q. How could LabMD have used these types of**
25 **guidelines to create a comprehensive information**

136

1 **security program at relatively low cost?**
2 A. They could have -- given their specific goals
3 and the types of information that they needed to
4 protect, they could have looked at the guidelines for
5 specific confidentiality goals and the types of
6 mechanisms that those guidelines recommend.
7 And so what those guidelines do, they provide
8 like a general and overall guidelines for like all
9 types of computing infrastructure. But if you have
10 additional things that differ, you are going to have to
11 evaluate that in a more process or in an approach and
12 really look at your structure to understand what in
13 addition to those guidelines you need to do.
14 **Q. How much would it cost to implement that**
15 **process-based approach?**
16 A. That process-based approach for a trained IT
17 person, that -- that takes people time in order to just
18 go through the process in evaluating the system and the
19 infrastructure.
20 **Q. So it's just a time cost then, not monetary?**
21 A. It's a time cost.
22 **Q. Professor Hill, I'd like to turn to the section**
23 **of your report that begins with paragraph 63.**
24 **Did complaint counsel ask you to provide an**
25 **opinion on whether LabMD used an appropriate set of**

197

1 power over those devices, the power to download software
2 and to change security settings.
3 So because these are multiuse environments
4 where they're reading their e-mail, they may
5 inadvertently open an attachment that has malicious
6 software embedded in it, any of those things put that
7 computer, any information that's stored on that
8 computer, at risk for exposure, so you would want to
9 store backups on a machine where those types of
10 activities are not occurring.
11 **Q. Did LabMD store backups on devices that were not**
12 **isolated from other employee activities?**
13 A. Yes.
14 **Q. Paragraph 104(e) of your report.**
15 **It says that a firewall should be configured to**
16 **block all unwanted traffic from entering the network.**
17 **Why is that important?**
18 A. That is important because if you restrict
19 communication that's initiated from outside for
20 unauthorized applications, then that would block that
21 traffic from entering your network.
22 **Q. What did you conclude about the configuration of**
23 **LabMD's firewalls?**
24 A. I concluded that LabMD's firewalls were not
25 configured to block all traffic that wasn't necessary

198

1 for LabMD to conduct its business.
2 **Q. Why did you reach that conclusion?**
3 A. I reached that conclusion because the Veritas
4 backup software had a port open, port 10,000, and the
5 Veritas backup software also had a vulnerability that
6 was a Level 5 vulnerability that gave an attacker
7 administrative access to that software and to the
8 machine that was running that software. There was no
9 business need for that port to be open. Backups were
10 done within the local area network and not across the
11 Internet.
12 **Q. Professor Hill, I'd like to turn back to CX 67,**
13 **page 22, and the top entry.**
14 **Is this the vulnerability that you were just**
15 **referring to?**
16 A. Yes.
17 **Q. In your opinion, if LabMD's firewalls had been**
18 **properly configured, would that have prevented the**
19 **LimeWire application on the billing manager's computer**
20 **from sharing files?**
21 A. No.
22 **Q. Why not?**
23 A. Because LimeWire can still share files even if
24 the request for files is not initiated from outside of
25 an organization's network.

199

1 If a computer that's using LimeWire within the
2 organization initiates a connection with the LimeWire
3 network, then data can be transferred to that computer
4 through that already-established communication channel.
5 **Q. How does the fact that a properly configured**
6 **firewall would not have prevented the LimeWire**
7 **application from sharing files relate to the importance**
8 **of a proper defense in depth strategy?**
9 A. It's a great example of why you need to use
10 defense in depth, because, as I stated earlier, it's an
11 arms race and applications become more and more
12 stealthy. If there's a mechanism in place, they try to
13 determine -- application -- malicious application
14 developers try to determine ways to circumvent that
15 mechanism to achieve its goal, and its goal is to gain
16 unauthorized access to a system.
17 So that's why you would need to deploy
18 mechanisms, heterogeneous mechanisms, in a layered
19 manner to combat that.
20 **Q. How did LabMD allowing the billing manager to**
21 **have an administrative account on her machine relate to**
22 **the LimeWire application being present on her computer?**
23 A. Given that the billings manager had
24 administrative access, the billings manager was able to
25 download and install applications onto the machine.

200

1 **Q. How long was the LimeWire application on the**
2 **billing manager's computer?**
3 A. The application was installed somewhere between
4 2005 and 2006. It was not removed until 2008.
5 **Q. Are there security measures that LabMD could**
6 **have used to detect the application sooner?**
7 A. Can you repeat the question, please.
8 **Q. Are there automated security measures that LabMD**
9 **could have used that would have detected -- could have**
10 **detected LimeWire before May 2008?**
11 A. Yes.
12 **Q. Can you give us and the court an example?**
13 A. They could have used a file integrity monitor
14 to detect the presence of the application.
15 **Q. What is a file integrity monitor?**
16 A. A file integrity monitor is an application that
17 first creates a base profile for your computer. And the
18 assumption when you create the base profile is that that
19 system is in a trustworthy state, so it actually creates
20 a list of all the files that's stored on your computer,
21 and periodically you can use it to check the integrity
22 of the computer.
23 And what I mean by "integrity" is determine
24 whether files have been added, the size of files have
25 changed, and those types of things.

201

1 And so when you -- when you do this integrity
2 check, by comparing the current state of the computer,
3 the current list of files, to the list of files that's
4 in your base profile, you can detect that there has
5 been a change.
6 A change doesn't necessarily mean that it is
7 malicious, but a change will help you to identify that,
8 you know, there's -- further investigation is needed,
9 and so you can further investigate those changes to
10 determine whether, for example, an unauthorized
11 file-sharing application has been downloaded.
12 JUDGE CHAPPELL: We're about at 5:30. What's
13 your status?
14 MS. LASSACK: I think that we could finish in
15 ten minutes or so, so...
16 JUDGE CHAPPELL: What do you think, Bailiff?
17 MR. MITCHELL: It's your call, sir.
18 JUDGE CHAPPELL: Press on.
19 BY MS. LASSACK:
20 **Q. Professor Hill, did LabMD use file integrity**
21 **monitoring?**
22 A. No.
23 **Q. Could LabMD have corrected its failure to use**
24 **readily available measures to prevent or detect**
25 **unauthorized access to personal information on its**

202

1 **network at relatively low cost?**
2 A. Yes.
3 **Q. How could LabMD have done that?**
4 A. LabMD could have enforced a policy that
5 prevented employees from having administrative access.
6 They could have used file integrity monitoring
7 software that was freely available.
8 **Q. How much would it have cost to prevent employees**
9 **from having administrative accounts?**
10 A. Nothing. It would only cost people time, so no
11 additional monetary cost.
12 **Q. How much would it have cost to store backups of**
13 **personal information on machines that weren't used for**
14 **other employee purposes?**
15 A. There were other machines like servers
16 available, so no additional machines would need to be
17 purchased.
18 **Q. Professor Hill, earlier this afternoon, you**
19 **said no -- there's no such thing as perfect security.**
20 **And His Honor asked whether this means that there is**
21 **always the likelihood of a security problem. Do you**
22 **recall that testimony?**
23 A. Yes.
24 **Q. If a company that maintains personal**
25 **information cannot achieve perfect security, what, in**

203

1 **your opinion, should be a company's goal with regard to**
2 **its security?**
3 A. The company's goal is to do what is reasonable
4 and appropriate and to apply strategies that would limit
5 the probability of compromise.
6 **Q. Professor Hill, now that we've discussed all of**
7 **your specific opinions about LabMD's security practices,**
8 **I'd like to turn back to your overall conclusion about**
9 **LabMD's security practices.**
10 **What is your overall conclusion about the**
11 **reasonableness and appropriateness of LabMD's security**
12 **practices?**
13 A. My overall conclusion is that LabMD did not
14 practice reasonable and appropriate security to ensure
15 the protection of its infrastructure and its data.
16 **Q. What time period does that conclusion cover?**
17 A. January 2005 until July 2010.
18 **Q. Do you offer any opinion about the**
19 **reasonableness of LabMD's security practices after**
20 **July 2010?**
21 A. No, I do not.
22 **Q. Could LabMD have corrected its security failures**
23 **at little or no cost?**
24 A. Yes.
25 MS. LASSACK: Your Honor, that's my final

204

1 question.
2 JUDGE CHAPPELL: All right. Thank you.
3 MS. LASSACK: I would like to move admission of
4 CDX 01, which is the version of the IT employee timeline
5 that was not discussed with Professor Hill. And I'd
6 also like to move the admission of CDX 02.
7 JUDGE CHAPPELL: Any objection?
8 MR. SHERMAN: Yes. I was informed that this
9 was a demonstrative exhibit and not something that was
10 going to be admitted into evidence, so I would object
11 on that basis. I thought this was a demonstrative.
12 MS. LASSACK: Well, it's also a summary without
13 Professor Hill's markup, which is what I would move
14 first, CDX -- sorry -- CXD 01, which is a summary
15 exhibit of testimony, which I believe we established the
16 foundation for with Professor Hill's testimony.
17 I also have here binders with testimony that
18 supports the summary exhibit that is CXD 1, the LabMD IT
19 employee timeline.
20 And I'd also like to move a third exhibit, which
21 is the LabMD IT employee timeline with Professor Hill's
22 markup, which we'll give a new --
23 JUDGE CHAPPELL: Okay. What's the first exhibit
24 you're offering?
25 MS. LASSACK: So the first exhibit would be

In the Matter of:

LabMD, Inc.

May 21, 2014
Trial - Public & In Camera Record
Volume 2

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION

I N D E X

IN RE LABMD, INC.

TRIAL VOLUME 2

PUBLIC AND IN CAMERA RECORD

MAY 21, 2014

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
HILL		214	311	319	
			324		
WILMER	331	352			
KAM	377				

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
(none)				
JX				
(none)				

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 21, 2014
9:37 a.m.
TRIAL VOLUME 2
PUBLIC AND IN CAMERA RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
MARGARET LASSACK, ESQ.
RYAN MEHM, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
HALLEE MORGAN, ESQ.
MICHAEL PEPSON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

230

1 **negative impact or consequences of these**
2 **vulnerabilities; is that correct?**
3 A. I specified some.
4 **Q. You specified some but not all.**
5 A. Not all.
6 **Q. Is there any evidence in your review of the**
7 **record that any of these consequences that you specified**
8 **occurred at LabMD?**
9 A. There's no evidence to support that, and as I've
10 previously stated, there were no such data logs that
11 will allow me to make such a conclusion.
12 **Q. Dr. Hill, yesterday you also testified that in**
13 **arriving at your conclusions, you looked at standards in**
14 **the industry to determine whether or not LabMD's data**
15 **security met those standards; is that a fair statement**
16 **with regard to your testimony?**
17 A. I think a more accurate statement would be, is
18 that I based my opinions on my knowledge within the area
19 and I supported my conclusions with the standards and
20 guidelines that I used.
21 **Q. And you indicated that you looked at government**
22 **standards and guidelines; is that correct?**
23 A. Yes.
24 **Q. And did you look at FTC standards and guidelines**
25 **for data security?**

231

1 A. I did not consider the FTC standards and
2 guidelines.
3 **Q. Did you look at HIPAA -- and do you know what**
4 **HIPAA is?**
5 A. Yes, sir, I do.
6 **Q. Okay. And would you agree that HIPAA is a**
7 **regulation that governs the -- in part, governs the**
8 **storage and transfer of health-related information by**
9 **medical care providers?**
10 A. I can't make a statement or -- about the legal
11 aspects of HIPAA and what it governs. I don't
12 understand the legal aspects of what it governs.
13 **Q. So you're not intimately familiar with HIPAA**
14 **then.**
15 A. No, sir.
16 **Q. Okay. And you did not consider HIPAA or HIPAA's**
17 **guidelines in the formulation of your opinion in this**
18 **case; correct?**
19 A. I considered the HIPAA security rule portion.
20 **Q. And that's all with regard to HIPAA?**
21 A. Yes.
22 **Q. And so it didn't play into your consideration or**
23 **your opinion as to whether or not LabMD was a**
24 **HIPAA-covered entity.**
25 A. No. I didn't take that into consideration.

232

1 **Q. Can we pull up Appendix B to the report of**
2 **Ms. Hill, please.**
3 A. Excuse me, Mr. Sherman.
4 **Q. Yes.**
5 A. There was also -- there were, as part of the
6 HIPAA documents, the six basic rules for risk
7 assessment, and that was also a HIPAA document that I
8 used.
9 **Q. Professor Hill, you indicated that you**
10 **considered government standards in formulating your**
11 **opinion; is that correct?**
12 A. Yes.
13 **Q. And I believe one of the government standards**
14 **that you considered was NIST? And I won't ask you what**
15 **that stands for since I think we established that**
16 **yesterday through much wrangling.**
17 **But you did consider NIST; is that correct?**
18 A. Yes. The 800-30 document from NIST.
19 **Q. Was there any specific portion of NIST that you**
20 **considered to be relevant to LabMD's data security?**
21 A. That particular document talks about risk
22 assessment practices, and yes, I considered that.
23 **Q. How big is the NIST document that you**
24 **considered?**
25 A. I don't recall that.

233

1 **Q. Is it voluminous?**
2 A. Voluminous?
3 **Q. Yes.**
4 **Does it contain hundreds of pages?**
5 A. No. I don't recall that it contains hundreds of
6 pages, no.
7 **Q. And so in looking at NIST, you looked at it as**
8 **part of an overview and not in depth; would that be a**
9 **fair statement?**
10 A. Yes. I was just looking at the specific
11 guidelines that they provided to support the conclusions
12 that I'd already made.
13 **Q. And is it fair to say that you did the same for**
14 **all of the other government standards that are listed in**
15 **Appendix B to your report, that you looked at them as an**
16 **overview to support what you already knew? Is that**
17 **correct?**
18 A. Yes. I was trying to find documents that
19 provided guidelines for security, and those documents
20 align with the recommendations that I made for a
21 comprehensive information security plan that was
22 reasonable and appropriate. Yes.
23 **Q. So is it fair to say that the process you used**
24 **for coming up with your conclusion began with a review**
25 **of the evidence in the record in this case? Is that**

234

1 **correct?**
2 A. Yes.
3 **Q. Based on that review and based on your**
4 **knowledge, you then came to your conclusion with regard**
5 **to LabMD's data security; is that correct?**
6 A. Yes.
7 **Q. And then you went out in search of standards and**
8 **guidelines to support what you already knew.**
9 A. I found documents. And I don't think it was a,
10 you know, big search for documents. These are
11 documents that IT professionals use for guidance, and
12 so...
13 **Q. You testified yesterday that these were**
14 **standards and guidelines in the industry; correct?**
15 A. What do you mean by "in the industry"?
16 **Q. That was my next question to you.**
17 **When you testified that these are industry**
18 **standards, what industry were you talking about?**
19 A. With regards to industry and government
20 standards, the industries relating to computer security
21 and information technology professionals. That's the
22 industry.
23 **Q. So you were not referring to, in your**
24 **testimony, industry standards for medical care**
25 **providers.**

235

1 A. There's a specific document that I cite from
2 the National Research Council that does provide
3 guidelines for protecting medical data, and those
4 guidelines are consistent with protection mechanisms
5 that are recommended by the other standards, so they're
6 consistent.
7 When you want to protect infrastructure, there
8 are some common guidelines that are across all types of
9 domains. Computing is pervasive, so these guidelines,
10 whether they're from NIST or from the Computer Emergency
11 Response Team or from the National Research Council that
12 specifically focused on medical data, they have
13 consistent guidelines. And that's because computing is
14 pervasive and consistent across different types of
15 business domains.
16 **Q. And so you considered all of these sources to**
17 **the exclusion of HIPAA and to the exclusion of anything**
18 **out there that was available discussing data security**
19 **standards from the FTC; is that correct?**
20 A. I don't quite understand your question. Can you
21 restate it.
22 **Q. It's just that I want to make sure I'm getting**
23 **your testimony correct, that in reviewing standards and**
24 **guidelines for data security to assist in the**
25 **formulation or to support the formulation of your**

236

1 **opinion, you didn't consider the guidelines set out by**
2 **HIPAA, other than the security rule and the six**
3 **principles of risk assessment, and you didn't consider**
4 **any information that was out there with regard to**
5 **standards for data security from the FTC.**
6 A. Yes, that is correct.
7 **Q. Professor Hill, did you review the complaint in**
8 **this case prior to formulating your opinion?**
9 A. Yes.
10 **Q. And so are you familiar with the allegations in**
11 **paragraph 10 of the complaint?**
12 **And we can put them on the screen for you.**
13 **Would that help?**
14 A. Yes. But let me back up. I think I misstated.
15 I began reviewing the documents before I ever
16 saw this complaint, and so I didn't formulate my
17 opinions after seeing the complaint, so I misstated. I
18 apologize.
19 **Q. When did you start reviewing the documents in**
20 **this case, approximately?**
21 A. I started reviewing the documents -- it was
22 either June or July of 2013. And I -- I'm thinking more
23 it's July, and I think I made that statement in the --
24 during the deposition, but I think it's July.
25 **Q. And how long after you began reviewing the**

237

1 **documents did you see the complaint for the first time?**
2 A. I think that I saw the complaint much later. I
3 recall seeing the complaint as I was preparing my expert
4 document, so that's when I recall seeing it.
5 **Q. And so if you look at -- can you see the screen?**
6 A. Yes, I can.
7 **Q. If you look at paragraph 10 subparagraph (a).**
8 A. Yes.
9 **Q. It reads "did not develop, implement or maintain**
10 **a comprehensive information security program to protect**
11 **consumers' personal information."**
12 **Did I read that correct?**
13 A. Yes.
14 **Q. Now, you use that phrase "comprehensive**
15 **information security program" in your report; correct?**
16 A. Yes.
17 **Q. Who coined that phrase? Was that you or did you**
18 **look at the complaint and put that in your report?**
19 A. I think we've discussed this before, but the --
20 that phrase is in some form of the concept of a
21 comprehensive information security program is
22 well-known, and that -- so the concept is known. The
23 exact phrase, as I've stated previously, I don't recall
24 if -- if, you know, I stated it or they stated it.
25 But I was asked to assess LabMD's security

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

306

1 THE WITNESS: "Defense in depth" is a term
2 that's used in the IT community and -- and it is my
3 understanding that it was originally taken from
4 military strategy, but it has been adopted by the IT
5 community to explain the most effective way to deploy
6 mechanisms.
7 JUDGE CHAPPELL: When do you believe you first
8 saw that use of that phrase as commonplace in the
9 IT community?
10 THE WITNESS: I --
11 JUDGE CHAPPELL: I mean, you don't have to --
12 like five years, ten years, one year, how long ago?
13 THE WITNESS: I think that it was maybe around
14 five years ago or so when I became familiar with the
15 strategy.
16 JUDGE CHAPPELL: And the seven principles
17 you've talked about, is that your formulation? Even
18 though I think you said they were drawn from various
19 literature or guidelines, did you formulate the seven
20 principles?
21 THE WITNESS: No, sir. These are principles
22 that I've learned through my experience. And these are
23 consistent with what may be found in the guidelines
24 that are provided by some of the resources that I cite.
25 JUDGE CHAPPELL: Did I hear you say earlier that

307

1 you generally won't find all seven if you look at
2 guidelines or information?
3 THE WITNESS: You may not find all seven
4 specifically. You may find six, excluding the
5 "don't keep what you don't need," because since the
6 management of large amounts of data is an emerging
7 trend, then this is becoming more of a needed principle
8 because of that, because organizations are keeping
9 large amounts of money, so you may not see that
10 particular principle in some of the documents that I
11 cite.
12 JUDGE CHAPPELL: Is it your opinion that
13 respondent's data was unreasonable or inadequate simply
14 because it didn't meet standards for defense in depth?
15 THE WITNESS: I feel that it was because not
16 just because it didn't meet standards for defense in
17 depth but because they were not comprehensive and that
18 they had vulnerabilities that were not being addressed
19 because of the lack of specific policies and enforcement
20 mechanisms.
21 JUDGE CHAPPELL: Just so I'm clear, defense in
22 depth, does that require a company to meet the seven
23 principles?
24 THE WITNESS: Defense -- it doesn't require the
25 companies to meet the seven principles, but it's more

308

1 of a strategy about how to deploy mechanisms within
2 your computing infrastructure, mechanisms and policies,
3 in order to satisfy your security goals.
4 So you have this comprehensive information
5 security plan that lists out, you know, what mechanisms
6 will enforce your policies and satisfy your security
7 goals, but defense in depth talks about you need a
8 heterogeneous set of mechanisms, not the same. You need
9 to deploy them at multiple layers in your network in
10 order for them to be effective.
11 So that's what defense in depth says --
12 JUDGE CHAPPELL: So -- go ahead.
13 THE WITNESS: -- so --
14 JUDGE CHAPPELL: I didn't mean to interrupt you.
15 Go ahead.
16 THE WITNESS: Okay.
17 So you have this plan that you devise via a
18 process of kind of a balancing process where you look at
19 your goals and look at the highest risks and
20 vulnerabilities, and you identify mechanisms that will
21 address those that you're more likely to encounter with
22 regards to the risk and the vulnerabilities that would
23 be exploited. And then given that, you want to then
24 deploy those mechanisms in a defense in depth way.
25 So that's how defense in depth kind of fits with

309

1 this comprehensive information security program.
2 JUDGE CHAPPELL: So if I understand correctly,
3 defense in depth would be considered the gold standard
4 in the industry.
5 THE WITNESS: I wouldn't say that defense in
6 depth is a gold standard. It's an effective strategy.
7 JUDGE CHAPPELL: I think it's paragraph 52 of
8 your expert report says -- you're talking about best
9 practices that would include seven principles. And I'm
10 just trying to follow you here.
11 If someone follows the seven principles, are
12 they meeting what you would consider defense in depth,
13 that requirement?
14 THE WITNESS: If someone follows those seven
15 principles and deploy mechanisms at the various levels
16 within their infrastructure, then they would satisfy
17 defense in depth.
18 JUDGE CHAPPELL: And again so I'm clear, is
19 defense in depth, in your opinion, the exercise of
20 utmost care, in other words, above reasonable care?
21 THE WITNESS: I'm sorry, Your Honor. Could you
22 repeat.
23 JUDGE CHAPPELL: Defense in depth, is that
24 exercising reasonable care or is it more likely what you
25 would call or consider utmost care?

310

1 THE WITNESS: I would say it's reasonable, sir.
2 JUDGE CHAPPELL: So in your opinion then,
3 reasonable care would be defense in depth for your
4 network.
5 THE WITNESS: Reasonable care would be defense
6 in depth.
7 JUDGE CHAPPELL: Okay. Thank you.
8 We will take our lunch break.
9 How much time do you think you'll need for
10 redirect?
11 MS. LASSACK: Under half an hour, probably
12 closer to 15 minutes.
13 JUDGE CHAPPELL: Okay. We'll reconvene at
14 2:10 p.m.
15 We're in recess.
16 (Whereupon, at 1:03 p.m., a lunch recess was
17 taken.)
18
19
20
21
22
23
24
25

311

1 A F T E R N O O N S E S S I O N
2 (2:12 p.m.)
3 JUDGE CHAPPELL: Back on the record.
4 Redirect?
5 MS. LASSACK: Thank you, Your Honor.
6 - - - - -
7 REDIRECT EXAMINATION
8 BY MS. LASSACK:
9 **Q. Good afternoon, Professor Hill.**
10 A. Good afternoon.
11 **Q. I'd like to start by directing your attention to**
12 **paragraph 91 of your expert report, which is labeled**
13 **CX 740, and which begins on page 35.**
14 **Mr. Sherman asked you this morning about the**
15 **subparagraphs of paragraph 91, which begin on the**
16 **following page, page 92. Do you remember that?**
17 A. Yes.
18 **Q. To clarify the record, the opinions in**
19 **paragraphs 91 (a) through (g) of your report are true**
20 **for what time period?**
21 A. Prior to 2010.
22 **Q. Professor Hill, you testified this morning about**
23 **intrusions. Do you recall that testimony?**
24 A. Yes.
25 **Q. In giving that testimony, how are you defining**

312

1 **the word "intrusion"?**
2 A. The way that I'm defining the word "intrusion"
3 is that an intrusion is unauthorized access that
4 originates from outside of a network.
5 **Q. When you say "unauthorized," unauthorized from**
6 **whose perspective?**
7 A. Unauthorized from the perspective of the
8 organization.
9 **Q. Professor Hill, you also testified this morning**
10 **that there were not sufficient logs to show how the**
11 **1718 File left LabMD. Do you recall that testimony?**
12 A. Yes.
13 **Q. Would you please explain to the court what you**
14 **mean by that.**
15 A. There were no -- there was no information
16 regarding the data communication that occurred that
17 allowed that file to leave the network.
18 For example, if you had mechanisms in place to
19 capture the data across the network, then you could
20 possibly have information that would be able to tell you
21 how the file left the network.
22 So when I say "logs," I'm talking about
23 information, data communication information, the data
24 that transferred between the external entity and LabMD's
25 network.

313

1 **Q. So that information was not available in this**
2 **case?**
3 A. No, it was not available.
4 **Q. Professor Hill, you testified this morning about**
5 **certain LabMD policies and LabMD's employee manual. Do**
6 **you recall that testimony?**
7 A. Yes.
8 **Q. In your expert opinion, is it reasonable to**
9 **expect employer policies like the ones you testified**
10 **about this morning to be followed to the letter?**
11 A. It's not reasonable to expect them to be
12 followed to the letter.
13 **Q. Why not?**
14 A. Because there can always be human error.
15 And so the human is the weakest part of any
16 security plan, and so there could be a misunderstanding
17 of the policy, there could be misconfigurations of
18 mechanisms, and so there can always be an unintentional
19 mistake on the part of the human that would prevent a
20 policy from being followed to the letter. I think it's
21 unreasonable to expect that.
22 **Q. Professor Hill, you also testified this morning**
23 **that a company should be able to specify what types of**
24 **information that its employees have access to. Do you**
25 **recall that testimony?**

406

1 that were disclosed also.
2 So that's the first factor.
3 **Q. Can you please go on to describe briefly the**
4 **other three factors.**
5 A. Yeah. The other three factors include the --
6 to whom the disclosure was made, was this another
7 employee perhaps, was the disclosure made to another
8 employee, perhaps in the same institution, or was it
9 disclosed the another consumer perhaps or even an
10 identity thief.
11 The third is, was this information accessed and
12 viewed by these individuals.
13 And the fourth is what risk mitigation is taking
14 place in order to reduce the risk of harm to these
15 consumers.
16 **Q. And what are these four factors derived from?**
17 A. Primarily from my experience working with
18 other -- our clients, as well as working with other
19 privacy professionals who deal with data breaches,
20 you know, within their own organizations.
21 **Q. And anything else?**
22 A. You know, there may be some specific guides
23 that have been published by various organizations over
24 the last several years.
25 The issue of risk of harm is so central to the

407

1 analysis and the planning once a disclosure is made,
2 it -- it's -- it's central to all discussions that we as
3 privacy professionals have when we're trying to
4 determine what will happen or what could happen to
5 individuals once their unauthorized -- or once their
6 sensitive personal information is disclosed.
7 **Q. And why did you use this approach, Mr. Kam?**
8 A. When the FTC asked me to do an analysis, I
9 wanted to be sure that others in my profession who
10 could be asked to do something similar would arrive at
11 a similar assessment of risk. And therefore, I looked
12 at a way to make it simple or simpler to understand
13 what is a relatively complex and subjective assessment,
14 and therefore, I used four factors to describe this in
15 my report.
16 **Q. Mr. Kam -- excuse me. Court's indulgence.**
17 **(Pause in the proceedings.)**
18 **Is part of the reason, Mr. Kam, that you used**
19 **this methodology or approach so that others could test**
20 **your method?**
21 A. Yes.
22 **Q. Mr. Kam, I'd like to ask you some questions now**
23 **about the exposure of the 1718 File that you refer to in**
24 **your report as the P2P disclosure.**
25 **What is the 1718 File?**

408

1 A. It's a file indicated by the name that I
2 received called the insurance aging file and includes
3 the sensitive personal information of approximately
4 9300 consumers.
5 **Q. And who did this file belong to?**
6 A. According to the information I received and
7 reviewed, it belonged to LabMD.
8 **Q. And where, where was the 1718 File found?**
9 A. According to Robert Boback's testimony, it was
10 first found on February 5, 2008 by his company,
11 Tiversa.
12 **Q. And where did Tiversa find the file in**
13 **February of 2008?**
14 A. Again, according to Robert Boback's testimony,
15 it was found on a peer-to-peer network.
16 **Q. Was the file found after that?**
17 A. Yes.
18 **Q. How many times after February 2008 was the file**
19 **found?**
20 A. It was found several times.
21 It was found on November 5, 2008.
22 It was again found on April 7, 2011.
23 It was again found on June 9, 2011 and yet
24 again just before Robert Boback testified in
25 November 2013.

409

1 **Q. In what format was the 1718 File discovered?**
2 A. It was discovered in clear text, meaning anyone
3 who had access to a peer-to-peer network could view this
4 information.
5 **Q. What else was found at the locations where the**
6 **1718 File was found?**
7 A. Robert Boback in his testimony also stated that
8 there was information that could be used to commit
9 identity theft --
10 JUDGE CHAPPELL: I have a question here. Excuse
11 me, Mr. Kam.
12 THE WITNESS: Yes, sir.
13 JUDGE CHAPPELL: Are you asking this witness to
14 insert facts into the record or are you asking him this
15 because this is what he based his opinion on? Because
16 his factual assertions here are not going to have any
17 merit in the record.
18 MR. MEHM: I'm asking these questions,
19 Your Honor, because they are central to the methodology
20 that Mr. Kam used, which we are going to move to very
21 shortly, to discuss his analysis of the risk of harm
22 from this particular instance, so these facts are
23 critical, as Mr. Kam will testify about momentarily, to
24 his analysis.
25 JUDGE CHAPPELL: So if I understand this, he

410

1 based a lot of his opinions on Mr. Boback's testimony.
2 BY MR. MEHM:
3 **Q. Mr. Kam, could you address that.**
4 A. Yes. Yes, sir.
5 So for the P2P incident specifically, the answer
6 is yes.
7 JUDGE CHAPPELL: All right. Thank you.
8 BY MR. MEHM:
9 **Q. And I'm sorry. Let me just look here at the**
10 **screen.**
11 **Mr. Kam, did you get a chance to respond to --**
12 **just -- excuse me. Court's indulgence.**
13 **(Pause in the proceedings.)**
14 **In your experience, Mr. Kam, do identity thieves**
15 **or medical identity thieves look for information on**
16 **peer-to-peer networks?**
17 A. Yes.
18 **Q. And what is your overall assessment of the risk**
19 **of harm to consumers based on the exposure of their**
20 **information in the 1718 File?**
21 A. My overall opinion is they are at significant
22 risk of harm to identity theft and medical identity
23 theft from the unauthorized disclosure of their
24 sensitive personal information.
25 **Q. And how did you conclude this?**

411

1 A. Using the four factors that we described or
2 that we touched on earlier, as well as the other
3 documents that the Federal Trade Commission provided.
4 **Q. And so let's turn now to those factors.**
5 **In applying the first factor, which you**
6 **testified a few moments ago encompasses the nature and**
7 **the extent of the information disclosed, what type of**
8 **information about consumers is contained in the**
9 **1718 File?**
10 A. Specifically in the 1718 File what I reviewed
11 included names, full name, first name, last name, middle
12 initial. It included dates of birth. It included full
13 nine-digit Social Security numbers. It included medical
14 diagnostic codes, CPT codes specifically, as well as
15 billing information and amounts.
16 Oh, and I should mention health insurance
17 numbers, health insurance addresses, health insurance
18 phone numbers and their addresses.
19 **Q. And how would you characterize generally the**
20 **sensitivity of this data?**
21 A. Generally it's very sensitive data. It could be
22 used to commit identity theft and medical identity
23 theft.
24 **Q. And why could this information be valuable to an**
25 **ID thief or a medical ID thief?**

412

1 A. It could be used to commit all -- many forms of
2 identity crimes, both for financial illicit gain as well
3 as to potentially cause embarrassment or for
4 reputational harm.
5 JUDGE CHAPPELL: Is medical ID theft
6 fraudulently procuring someone else's medical benefits?
7 THE WITNESS: Yes. Yes, sir.
8 BY MR. MEHM:
9 **Q. To what extent, Mr. Kam, does a consumer**
10 **generally change any of the information -- and I'm**
11 **talking about the sensitive consumer information -- that**
12 **was exposed in the 1718 File?**
13 A. You know, generally the information in that
14 particular file won't change. There will be
15 circumstances where an individual will change their
16 name. They'll change perhaps their insurance provider,
17 you know, but -- they may even change their address
18 multiple times moving from one place to another. But
19 the -- specifically the Social Security number and their
20 medical history won't change.
21 **Q. And does any of this information have a long**
22 **shelf life or live on for an extended period of time?**
23 A. Yes.
24 Specifically, Ryan, in the case of
25 Social Security numbers, unfortunately, research has

413

1 shown that identity thieves, if they don't use the
2 information themselves, will sell that data to an
3 average of eight other criminals.
4 In the case of health information, specifically
5 health insurance numbers, that information has a very
6 high street value in the black market, so whereas a
7 Social Security number or a credit card payment --
8 credit card number may be worth a dollar in the black
9 market, it's been shown or it's -- you'll see articles
10 reference health information may be worth $50 and
11 upwards of $500 to $1,000 on the black market.
12 **Q. Beyond what you just testified about a**
13 **Social Security number having a long shelf life, is**
14 **there any other categories of data that was contained in**
15 **the 1718 File that typically has a fairly long shelf**
16 **life?**
17 A. Well, essentially the consumer's health record,
18 their health information. If you're diagnosed with
19 prostate cancer or HIV or herpes or hepatitis, that
20 typically doesn't change.
21 **Q. Because some of this data has a long shelf life**
22 **and consumers rarely change it, can you describe how**
23 **consumers are at an ongoing risk of harm from the**
24 **disclosure of that information?**
25 A. Well, from the -- from identity theft, thieves

414

1 will continue to or will use that information to commit
2 identity crimes, whether it's, like I mentioned earlier,
3 setting up new accounts or using that person's
4 information for illicit financial gain.
5 In the case of health insurance information,
6 like Your Honor mentioned earlier, use of that
7 information -- or asked earlier about, use of that
8 information to defraud Medicare or Medicaid is a very
9 significant problem today to the tune of anywhere from
10 80 to 120 billion dollars is being defrauded out of the
11 Medicare and Medicaid systems today because of medical
12 identity fraud.
13 **Q. And why is it that consumers are at an ongoing**
14 **risk of harm from the exposure of this information that**
15 **has a long shelf life and that consumers rarely change?**
16 A. It's because this information is out and
17 available and it's impossible to make this information
18 private again, especially the health information.
19 MR. MEHM: Your Honor, I would request --
20 respectfully request that we go into an in camera
21 session at the end of Mr. Kam's examination to discuss
22 the 1718 File, which is CX 0010, which Your Honor
23 previously granted in camera status for.
24 In the in camera session, I also plan, with your
25 permission, to ask Mr. Kam about another document,

415

1 CX 0085, which you also previously granted in camera
2 status for.
3 JUDGE CHAPPELL: Okay. Just to clarify, are you
4 asking for in camera now or are you giving me an
5 advisory warning?
6 MR. MEHM: A heads-up.
7 JUDGE CHAPPELL: So not at this time.
8 MR. MEHM: Not at this time.
9 JUDGE CHAPPELL: Okay. And for future
10 reference, you don't have to tell me what the documents
11 are. I will trust you to know what's in camera. Just
12 ask me for the in camera session.
13 So we're not there yet.
14 MR. MEHM: That's correct, Your Honor.
15 JUDGE CHAPPELL: All right. Let me know.
16 MR. MEHM: Okay. I will. Thank you.
17 BY MR. MEHM:
18 **Q. Mr. Kam, let's turn now to the second and third**
19 **risk factors.**
20 **In assessing those factors -- and you testified**
21 **earlier that is to whom the disclosure was made and**
22 **whether the information was acquired and viewed -- what**
23 **information did you consider?**
24 A. You know, I considered, again, the testimony
25 from Robert Boback, where he stated that that

416

1 information was found -- the information in the
2 1718 File specifically was found at four IP addresses.
3 **Q. And were there other elements that you**
4 **considered from Mr. Boback's testimony regarding the**
5 **second and third factors?**
6 A. Yes. It had -- there was I believe at one of
7 those four IP addresses a suspect who was arrested by
8 federal law enforcement who was suspected of committing
9 identity theft.
10 MS. MORGAN: Objection, Your Honor.
11 JUDGE CHAPPELL: Basis?
12 MS. MORGAN: The witness does not have personal
13 knowledge of this incident. He doesn't know -- he
14 doesn't have personal knowledge of whether anyone was
15 arrested in connection with an IP address.
16 MR. MEHM: Your Honor, Mr. Kam testified that he
17 based his assessment of this -- of these two risk
18 factors on Mr. Boback's testimony and there is
19 information to that effect in the transcript of
20 Mr. Boback.
21 JUDGE CHAPPELL: Well, the way I read this, he
22 was asked what other elements he considered. He told us
23 something he believed. I would think that would be
24 something you would want to inquire into in cross rather
25 than objecting at this time.

417

1 Do you withdraw your objection?
2 MS. MORGAN: Your honor, as long as it's clear
3 in the record that that came -- that he drew that fact
4 from Mr. Boback's testimony, then I will withdraw my
5 objection.
6 JUDGE CHAPPELL: I think that's clear based on
7 the form of the question.
8 Go ahead.
9 MR. MEHM: Yeah. Thank you, Your Honor.
10 BY MR. MEHM:
11 **Q. Turning to factor four, Mr. Kam -- and that, as**
12 **you testified earlier to, deals with the mitigation of**
13 **risk -- to what extent could consumers have mitigated**
14 **the risk of identity theft or medical identity theft**
15 **created by the unauthorized disclosure of their personal**
16 **information in the 1718 File?**
17 A. You know, as I mentioned earlier, consumers
18 have no way of knowing when an organization has a
19 disclosure unless they are notified by the organization
20 that had the breach.
21 In this case, my reading of Michael Daugherty's
22 testimony stated -- where he stated that they
23 decided -- LabMD decided not to go to notification;
24 therefore, these consumers, these 9300 consumers, whose
25 information was disclosed, whose sensitive personal

In the Matter of:

LabMD, Inc.

May 23, 2014
Trial - Public & In Camera Record
Volume 4

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION

I N D E X

IN RE LABMD, INC.

TRIAL VOLUME 4

PUBLIC AND IN CAMERA RECORD

MAY 23, 2014

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
VAN DYKE		664	708		
JOHNSON	749	793	801		
SHIELDS	809	889	922	924	

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
Number529		708		
JX				
(none)				

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 23, 2014
9:31 a.m.
TRIAL VOLUME 4
PUBLIC AND IN CAMERA RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
KATHERINE M. SANTMYER, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

664

1 P R O C E E D I N G S
2 - - - - -
3 JUDGE CHAPPELL: Let's go back on the record
4 Docket 9357 as we start the very long day.
5 I think we were in the middle of cross?
6 MR. SHERMAN: That's correct, Your Honor.
7 JUDGE CHAPPELL: Go ahead.
8 MR. SHERMAN: Thank you, sir.
9 - - - - -
10 Whereupon --
11 JIM VAN DYKE
12 a witness, called for examination, having been
13 previously duly sworn, was examined and testified
14 further as follows:
15 CROSS-EXAMINATION
16 BY MR. SHERMAN:
17 **Q. Good morning, Mr. Van Dyke.**
18 A. Mr. Sherman.
19 (Pause in the proceedings.)
20 JUDGE CHAPPELL: All right.
21 MR. SHERMAN: Thank you, Your Honor.
22 BY MR. SHERMAN:
23 **Q. Mr. Van Dyke, if you could turn to page 8 of**
24 **your report, which is I believe where we were yesterday**
25 **when we left off.**

665

1 **Are you there, sir?**
2 A. I am.
3 **Q. So, Mr. Van Dyke, we were talking about**
4 **figure 1, and we were looking at the 30.5 percent figure**
5 **represented in the red bars in figure 1, and we were**
6 **talking about -- I think the phrase you used was**
7 **"cross-tabulation"?**
8 A. That's correct.
9 **Q. Okay. And what factors or facts were you**
10 **cross-tabulating to arrive at the 30.5 percent figure?**
11 A. So that 30.5 percent figure is the result of a
12 cross-tabulation or the intersection of two questions.
13 And in summary, those -- the first of the two questions
14 asks individuals if they have been notified of a data
15 breach, in this case in the previous twelve-month
16 period.
17 Secondly, in summary, or there's a question that
18 asks individuals if they have been the victim of
19 identity theft or what we've been calling identity fraud
20 committed in their name in the past twelve months.
21 **Q. And so those were the two factors**
22 **cross-tabulated and therefore represented in the**
23 **30.5 percent figure?**
24 A. That's correct.
25 **Q. So is the -- when we talk about the 30.5 percent**

666

1 **figure, how is that used with reference to either the**
2 **1718 File or the day sheets? And let's start with the**
3 **1718 File.**
4 **Does the 30.5 percent figure have any relevance**
5 **or relation to the 1718 File?**
6 A. To set the lay of the land, it absolutely does.
7 Now, we go on later in my expert report to take
8 a more precise estimate of the amount of the degree of
9 risk in quantitative terms represented by exposure of
10 the 1718 Files.
11 So the number is slightly different,
12 deliberately, yet in figure 1 here, we're -- the primary
13 purpose of this particular document was to show the
14 rising correlation between notification of a data breach
15 and individual incidents of identity fraud.
16 **Q. Was there anything that you reviewed in the**
17 **record that indicated to you that the individuals whose**
18 **names appeared on the 1718 File were notified of a data**
19 **breach?**
20 A. No.
21 **Q. And so the question then is, if the individuals**
22 **whose names appeared on the 1718 File were not notified**
23 **of a data breach, then how does the 30.5 percent figure**
24 **apply or have any relevance to the 1718 File?**
25 A. It has relevance to the 1718 File, that is, the

667

1 30.5 percent figure, because in the case of the field
2 of study on identity fraud, I use notification of a
3 data breach as the marker for exposure to a data
4 breach. And there's a very deliberate reason for that.
5 We are dealing with a crime in which the
6 perpetrator will deliberately conceal as much as they
7 can in order to be successful in making individuals
8 victims of fraud.
9 JUDGE CHAPPELL: Hold on a second.
10 (Pause in the proceedings.)
11 Go ahead.
12 MR. SHERMAN: Thank you, Your Honor.
13 BY MR. SHERMAN:
14 **Q. I still don't understand how the 30.5 percent**
15 **figure relates to those individuals whose names appear**
16 **on the 1718 File when those individuals were never**
17 **notified of a data breach.**
18 A. Perhaps I could have explained that more
19 clearly.
20 For identity fraud to be successfully
21 perpetrated by a criminal, there are two things that
22 have to happen, and we are measuring those two things
23 through every reliable method possible.
24 The first thing or act is unauthorized exposure
25 of PII. We have to get a reliable way of indicating

668

1 that that has happened.
2 Secondly, that fraud has happened in that same
3 individual's name, unauthorized transactions, that is.
4 So in calculating that 30.5 percent, we, in my
5 research, relied on a reliable method available to us,
6 which is asking individuals if they've been notified of
7 a data breach, so we knew that the data had been
8 exposed in that case, thing number one as I was
9 referring to it.
10 And the item -- the second category of the act
11 or thing, as I'm referring to it, was the unauthorized
12 transaction that that same individual experienced.
13 So in my research, we asked these same
14 individuals if they had experienced both things, the
15 data breach and the fraud. And what we found in our
16 calculation -- and I'll loop this back to the 1718 File
17 you asked about in just a moment -- but in the case of
18 my research, by asking people both of those questions,
19 the same individuals both questions, we were able to
20 divide the result of one question by the result of
21 another question to conclude that 30.5 percent of people
22 who had been notified of a data breach had identity
23 theft committed in their name.
24 That relates to the 1718 File because we know
25 that the 1718 File, from the testimony of Mr. Boback,

669

1 that it was found in four places where it didn't
2 belong, so that's the indicator of the first thing,
3 exposure of the data. And I use that to make an
4 estimate, a projection -- pardon me -- of the amount of
5 harm that those people who have had their data exposed
6 in an unauthorized way are likely to encounter.
7 **Q. So is it your conclusion that 30.5 percent of**
8 **the individuals whose names appear on the 1718 File will**
9 **or should experience identity fraud?**
10 A. It is close to that, so generally speaking,
11 yes, however, with an important qualification.
12 I use every opportunity I can to be as precise
13 as I can, so when I have more facts, such as in this
14 case I know exactly what information was exposed by
15 looking at the 1718 File that you're asking about, I
16 can see that there were Social Security numbers, a
17 particularly important record, exposed there.
18 By using my data to calculate the rate of fraud
19 experienced by people who have had their
20 Social Security number exposed, I come up with a very
21 similar but slightly different figure than the
22 30.5 percent.
23 **Q. What is that figure?**
24 A. That figure is -- and if you like, I can show
25 you where it's contained.

670

1 **Q. Please do. Well, show me where it is in your**
2 **report, the slightly different figure using those two**
3 **factors and applying them to the individuals and the**
4 **information found on the 1718 File.**
5 A. That is found on the bottom of page 11 in the
6 three bullets at the very bottom of the page where we,
7 rather than list that as an aggregate figure, the
8 30.5 percent, since that 30.5 is made up of three
9 individual types of identity fraud -- we could have
10 broken it out by type, just didn't want to make that
11 chart that has so much information too complicated --
12 on the bottom of page 11, in answer to your question,
13 we show the individual components that make up, if
14 added together, the comparable figure for just those
15 individuals who had their Social Security number, SSN,
16 exposed. And that would be 7.1 percent plus
17 7.1 percent plus 13.1 percent, in other words,
18 27.3 percent.
19 **Q. So if you add all of those percentages**
20 **together, you get 27.3 percent, which you're saying is**
21 **very close to your 30.5 percent figure; correct?**
22 A. That's correct.
23 **Q. And you come up with that figure based on your**
24 **calculations in figure 1; is that right?**
25 A. I wouldn't quite word it that way.

671

1 **Q. Yeah, help me out. I went into law because I**
2 **don't like math.**
3 A. I'm sorry. Could you repeat what you just said.
4 I was flipping pages.
5 **Q. Just help me out as to how you came to the**
6 **27.3 as a -- I think what you're saying, as a variable**
7 **or a variation on the 30.5 percent.**
8 JUDGE CHAPPELL: Although, in defense of people
9 who like numbers, a number of legal fields require
10 math.
11 MR. SHERMAN: That's why I'm standing before
12 you today, Judge.
13 THE WITNESS: So in answer to your question,
14 it's the exact same process. The process is identical.
15 It's just in the case of the figure shown on -- let me
16 restate that, please.
17 On page 8, the primary purpose of that image,
18 which shows a lot of different things, but it -- it is
19 intended to show the rising correlation over time of
20 data breach to identity fraud, that one is likely and
21 increasingly likely over the four years shown, one is
22 more likely to be correlated to the other.
23 The -- on page -- the figures shown on the
24 bottom of page 11 are used in identical way, but we are
25 able to take a more -- to apply a more precise use of

728

1 results of polling those individuals.
2 And also that, secondly, if I were to go out to
3 those individuals on the 1718 File and make an attempt
4 to contact them, I would imagine that some of them could
5 be contacted. Some of them might not be able to be
6 contacted. I just don't know what I would encounter in
7 that effort.
8 JUDGE CHAPPELL: Let's be honest about the
9 scope. You're not talking about contacting all of
10 them.
11 For example, you took the entire population of
12 the United States and surveyed, what, 9,000 people for
13 your survey?
14 THE WITNESS: 5,634, Your Honor.
15 JUDGE CHAPPELL: Okay. So it would be a mere
16 percentage, a small percentage, of the total number of
17 people on the 1718 File would need to be surveyed;
18 correct?
19 THE WITNESS: Unfortunately, I wish I could say
20 yes, but -- but the honest answer is no, and here's why,
21 is the difficulty -- there's a particular difficulty in
22 identity theft research that we've encountered for all
23 of our ten years. And it's best explained this way,
24 that because, thankfully, of the U.S. adult population,
25 in a typical year, only about one out of twenty

729

1 experience identity theft.
2 So when we have that one out of twenty, we have
3 to poll a lot of people to get a healthy sample.
4 You know, we can't just go out to, say, a hundred people
5 or -- and we found that we can't even stop at a
6 thousand, which is why we go to 5,000 minimum each year
7 now. And the only reason we do that is because of that
8 low incidence rate, the 5.4 percent.
9 We need to get to several hundred people who
10 have been a victim of fraud so we have statistical
11 accuracy, so we start to get an evened-out pattern, if
12 you will.
13 And then we further compound that by the fact
14 that we need to get a lot of people who would also say
15 they've had their information exposed, but -- again,
16 bear with me for just thinking that through
17 off-the-cuff -- by definition, the people in the
18 1718 File have had their information exposed, so let me
19 back up on my answer and say we would need to go with --
20 we would need to successfully contact a lot of people in
21 the 1718 File -- my off-the-cuff answer would probably
22 be well over a thousand -- to have good assurance that
23 we were dealing -- we had a quality sample that would
24 not have rough patterns to the result.
25 JUDGE CHAPPELL: So if I understand you right,

730

1 though, you and your company, you're all about this
2 Javelin survey. You're not so much in the business of
3 me bringing a stack of names to you and telling you to
4 conduct and create a survey; is that correct?
5 THE WITNESS: Yeah. We generally do not do
6 that.
7 JUDGE CHAPPELL: But if I wanted to hire someone
8 and say, Here's a stack with names on it, they could
9 create a survey and conduct it for me.
10 THE WITNESS: We do that for people. And we
11 have done that and we will continue to do that. That's
12 not -- that's not the majority of what we do. But yes,
13 we do that occasionally.
14 JUDGE CHAPPELL: Not that difficult, is it?
15 THE WITNESS: It's always difficult in that I
16 have to have statistical experts, but it brings in
17 unique challenges in that contacting people and
18 getting -- and solving for having the -- and not have --
19 I believe you mentioned the term "response bias" I
20 believe earlier -- ensuring that the pattern of those
21 who responded was not biased by the fact that the way in
22 which they responded didn't bias the pattern of
23 responses that I end up with.
24 And we have a very structured process in place
25 for my annual surveys. It's not simple, but I know

731

1 exactly what the issues are that I'll have to deal with
2 after having done this for ten years now with
3 5,000 people.
4 I would have to construct that by hand and
5 assemble a team do that. It actually would be quite a
6 challenge. It could be done, but it would be a
7 challenge.
8 JUDGE CHAPPELL: All right. Thank you.
9 THE WITNESS: Thank you.
10 JUDGE CHAPPELL: If the attorneys have any
11 questions regarding my questions, you may conduct them
12 on your redirect and, Mr. Sherman, on your recross.
13 MR. SHERMAN: Thank you, Your Honor.
14 MS. VANDRUFF: Thank you, Your Honor.
15 JUDGE CHAPPELL: Continue with your redirect.
16 MS. VANDRUFF: Thank you, Your Honor.
17 - - - - -
18 REDIRECT EXAMINATION (continued)
19 BY MS. VANDRUFF:
20 **Q. Mr. Van Dyke, you described for His Honor**
21 **Knowledge Networks and how you conduct the survey, the**
22 **identity fraud survey, but can you describe for**
23 **His Honor how the panels are selected.**
24 **That is, is it likely that His Honor is going to**
25 **receive an e-mail requesting that he complete the**

732

1 **identity fraud survey?**
2 A. His Honor as an individual, it's not likely that
3 he specifically would, because we are polling a small
4 section, in this case 5600 people out of 330 -- let's
5 just call it 300 perhaps U.S. adults, 300 million.
6 **Q. Mr. Van Dyke, are those 5600 people preselected**
7 **by Knowledge Networks?**
8 A. Yes, they are.
9 **Q. So it's not an e-mail blast that goes out on**
10 **behalf of Javelin to field the 2013 or any prior**
11 **identity fraud survey; is that correct?**
12 A. That -- that is correct. It is not a general
13 scattering. This is the opposite of that kind of a
14 loose polling method.
15 **Q. His Honor asked you questions about your**
16 **background in statistics.**
17 **Can you describe for the court, please, your**
18 **experience with respect to statistically and**
19 **methodologically valid surveys.**
20 A. Certainly.
21 So of my 30 years in the working world, the
22 last 15 have been spent in the field of research. And
23 in doing that, I have worked around structured
24 research, always gravitated toward that, especially
25 quantitative research more than qualitative by far.

733

1 And in doing that, I've -- I've personally designed
2 research surveys, which meant I've written out the
3 research questions.
4 I've gone back and forth with what are called
5 field houses. In this case, Knowledge Networks is known
6 to be about the highest-quality quantitative field house
7 there is.
8 That -- I've analyzed results of that
9 information. I'm known in my business to be a person
10 who will take data banners, you know, the spreadsheets
11 and tables and pull an all-nighter and literally not get
12 any sleep poring over the data fields.
13 I don't have a Ph.D. in statistics, and neither
14 do I claim to be a statistician. I'm not.
15 But I am drawn to this field of study because I
16 understand it, I love it, and I love the process of
17 discovery, and I communicate quite effectively I'm told
18 by people that do nothing but work in the field of
19 statistics.
20 **Q. And for how long have you been working in this**
21 **field?**
22 A. In the field of applied research, you know,
23 market research, for 15 years.
24 **Q. Yesterday, Mr. Van Dyke, His Honor asked you**
25 **whether it matters for the purposes of your analysis in**

734

1 **this case who receives personally identifying**
2 **information from an unauthorized disclosure.**
3 **Please explain briefly to the court why it's**
4 **your opinion that it does not matter who receives**
5 **personally identifying information from an unauthorized**
6 **disclosure for the purposes of calculating fraud**
7 **impacts.**
8 A. My position, Your Honor, is that it does not
9 matter what the identity is of the recipient of
10 unauthorized information because there is a single
11 overriding factor that matters so much that, quite
12 literally in this case, in my opinion, nothing else
13 matters. And that is was the individual who had access
14 to the information authorized or unauthorized to have
15 access to that information.
16 Because, in my opinion, if that individual who
17 had access to that information was not authorized to
18 have access, I therefore have a high degree of
19 confidence about what's likely to happen next on a
20 statistically significant basis.
21 **Q. Is that confidence driven from the survey data**
22 **that you've fielded for ten years?**
23 A. It absolutely is. That's where I'm going with
24 that. Thank you.
25 **Q. I'd like to direct your attention to your expert**

735

1 **report, Mr. Van Dyke, which has been marked as CX 0741,**
2 **and specifically to page 6 of your report.**
3 **Now, Mr. Sherman asked you a number of**
4 **questions about notification to the individuals who are**
5 **identified in the 1718 File. Do you remember those**
6 **questions?**
7 A. Yes, I do.
8 **Q. Okay. And does your expert report describe why**
9 **you nonetheless applied the data from the 2013 identity**
10 **fraud survey to the facts of the 1718 File disclosure?**
11 A. Yes, it does.
12 **Q. And why did you apply the 2013 data?**
13 A. Are you asking about the choice of the 2013 data
14 or why did I apply my survey process overall to the
15 1718 File?
16 **Q. Well, let's start with your survey process**
17 **overall.**
18 A. Okay. So the reason I applied my survey
19 process overall is because I have the benefit of having
20 the largest annual study really in the world that -- and
21 going out to now 5,000-plus people, where I can choose
22 these questions and change them from year to year based
23 on trends I'm seeing from a wide variety of places that
24 fraud technology are changing, use the highest-quality
25 deployment method, and I just can't get anything more

736

1 rigorous than that.
2 **Q. So then with respect to application of the**
3 **2013 data, why did you apply the 2013 data to the facts**
4 **of the 1718 File disclosure when no breach notification**
5 **had been provided?**
6 A. The reason I chose my 2013 survey results from
7 among the other years options I had available to me were
8 that -- and I'll paraphrase what I stated in the expert
9 report. Oh, I'm sorry. It's actually on page 7. Here
10 it is -- that consumers -- the point there under
11 item (c) in my expert report, consumers were notified of
12 the unauthorized disclosure of the day sheets in March
13 of 2013, which was within that same twelve-month period
14 my survey questions that we went over earlier were
15 asking about, and because in November 2013, Mr. Boback
16 testified that the insurance aging report, the
17 1718 File, could be found in multiple locations.
18 Those two incidents that I just referred to fall
19 within the period that I'd asked survey respondents
20 about within my most recent identity fraud survey
21 report.
22 **Q. And in your expert report, do you describe**
23 **whether or not data breach notification is a**
24 **prerequisite for a victim experiencing an increased risk**
25 **of harm?**

737

1 A. I do describe that.
2 **Q. Does that appear on page 6 of your report, sir?**
3 A. Yes, it does. It's at the bottom of page 6. My
4 words are: It is important to note that the notice is
5 not a prerequisite for a victim to experience an
6 increased risk of harm.
7 **Q. And so therefore, even though no data breach**
8 **notification was provided with respect to the**
9 **1718 File, your data is nonetheless applicable; is that**
10 **correct?**
11 A. Absolutely. We're really measuring whether or
12 not the data was known to have been exposed.
13 **Q. Mr. Sherman asked you about new account fraud,**
14 **existing card fraud and existing non-card fraud and**
15 **specifically referred you to the language in your**
16 **report at page 11 about consumers experiencing multiple**
17 **types of fraud. Do you recall that line of**
18 **questioning?**
19 A. I do.
20 **Q. Okay. And then -- well, just as a preliminary**
21 **matter, Mr. Van Dyke, is the methodology of the**
22 **identity fraud survey described in the survey document**
23 **itself?**
24 A. Yes.
25 **Q. Okay.**

738

1 A. It is.
2 **Q. And that's attached to your report as**
3 **attachment 1; is that correct?**
4 A. I believe that's what that attachment is
5 called.
6 **Q. Okay. Let me ask you to direct your attention,**
7 **please, to page 79 of the document that's been marked as**
8 **CX 741.**
9 MR. SHERMAN: Objection, Your Honor. I believe
10 this is beyond the scope of cross.
11 MS. VANDRUFF: May I respond, Your Honor?
12 JUDGE CHAPPELL: The best way to respond is with
13 the witness.
14 MS. VANDRUFF: Certainly.
15 JUDGE CHAPPELL: The witness needs to bring it
16 within the scope of the cross. That's how you respond
17 to that objection, not argument but witness testimony.
18 MS. VANDRUFF: I understand, Your Honor.
19 BY MS. VANDRUFF:
20 **Q. And Mr. Van Dyke, my apologies. I directed you**
21 **to page 79, but please to page 80 of the identity fraud**
22 **survey report, which is included within CX 741.**
23 **Do you describe in the third paragraph what you**
24 **do when an individual consumer reports multiple**
25 **categories of fraud occurring in his or her name?**

739

1 **(Pause in the proceedings.)**
2 A. I'm sorry. You're asking about the third
3 paragraph on page 7- --
4 **Q. The paragraph that begins "Many victims."**
5 A. I might be on -- is it page 79 in the lower
6 right that you're referring to of our methodology
7 statement?
8 **Q. Thank you, Mr. Van Dyke. No. I misspoke and I**
9 **asked you to turn your attention to page 80.**
10 A. 80. Okay.
11 **Q. Uh-huh.**
12 A. Great. Thank you.
13 **Q. Thank you.**
14 A. Oh, okay. Yes, I'm with you.
15 **Q. Okay. And how -- when Javelin is conducting**
16 **this study, what do you do when an individual consumer**
17 **reports multiple kinds of fraud conducted in his or her**
18 **name?**
19 A. We focus on the most serious crime. That's the
20 one that we count.
21 **Q. Okay. So then turning back to page 11 of your**
22 **report and the incidence rates that Mr. Sherman was**
23 **asking you about with respect to new account fraud,**
24 **existing non-card fraud and existing card fraud, is**
25 **there overlap in those rates?**

888

1 the Internet archive, and the Internet archive states
2 that it was retrieved in November of 2005, so we know it
3 was available as early as June of 2005.
4 **Q. I want to turn back to what we were talking**
5 **about earlier with respect to misconfigured peers and**
6 **ask, why would someone search for a misconfigured peer?**
7 A. Somebody would search for a misconfigured peer
8 in the hopes of finding information that other people
9 did not intend to share.
10 For example, you might be able to find a
11 misconfigured peer that shares personal documents,
12 things like tax documents, bank account information, any
13 other valuable or personal information that might be on
14 a computer that was accidentally exposed to the
15 peer-to-peer network.
16 **Q. And I want to go back one more time to**
17 **browse host. I know that we talked about it or that you**
18 **testified about W-9 Form being a way of getting access**
19 **to a sharing folder and then browsing that host.**
20 **What about people who search for music? Can**
21 **they use browse host as well?**
22 A. Absolutely. Somebody who is browsing and just
23 happened to look for a popular song that we might
24 suspect was on the computer, because we know the lab
25 manager was using the computer to search for music,

889

1 would also be able to use browse host, and that would
2 return the insurance aging or 1718 File as well.
3 **Q. Can you explain how the 1718 File could have**
4 **been inadvertently shared from LabMD's -- from the LabMD**
5 **billing manager's computer?**
6 A. Yes. It could have been inadvertently shared
7 when the LimeWire software was installed. Whoever
8 installed the LimeWire software would have chosen the
9 My Documents folder to share, which exposed all the
10 information of files that are placed in that directory.
11 MR. SHEER: With your indulgence, please.
12 (Pause in the proceedings.)
13 I have no further questions.
14 JUDGE CHAPPELL: Cross?
15 MR. SHERMAN: Yes, Your Honor.
16 - - - - -
17 CROSS-EXAMINATION
18 BY MR. SHERMAN:
19 **Q. Professor Shields.**
20 A. Yes, sir.
21 **Q. My name is William Sherman. We haven't met, but**
22 **I represent LabMD.**
23 **I'm going to ask you a few questions about some**
24 **of the questions that you were being asked by**
25 **Mr. Sheer.**

890

1 **Some of the most recent questions or some of**
2 **the last ones he asked you were about some articles**
3 **that you cited in your report. I guess one was dated**
4 **2005 and the other one was from the SANS Institute.**
5 **Do you recall those articles?**
6 A. Yes, sir. We only talked about a couple of
7 articles. There are other articles that are referenced
8 in my expert report.
9 **Q. I understand that.**
10 A. Okay.
11 **Q. You're not suggesting that LabMD was not aware**
12 **of the dangers of peer-to-peer file sharing, are you?**
13 A. I'm not aware of what LabMD was or was not aware
14 of. I am aware that the resources to find out about the
15 dangers of peer-to-peer file sharing were available
16 online to anybody who looked.
17 **Q. Okay. So when you reviewed, quote-unquote, the**
18 **record in formulating your opinion, you didn't look at**
19 **LabMD's Employee Handbook or some of their written**
20 **policies concerning what employees should and should not**
21 **be doing?**
22 A. No, sir. I wasn't asked to consider that.
23 **Q. Were you aware that LabMD employees were told**
24 **that they should not download programs off the**
25 **Internet?**

891

1 A. I believe Mr. Fisk makes that assertion in his
2 report.
3 **Q. But you didn't find it independently outside of**
4 **Mr. Fisk's report when you were reviewing documentation**
5 **for your opinion.**
6 A. I'm trying to recall. I reviewed a number of
7 documents.
8 I believe the copy of the handbook was in the
9 documents that I reviewed. However, I was not asked to
10 offer an opinion about the policies of LabMD, so I did
11 not look into them in detail.
12 **Q. Okay. During the questioning, you were shown**
13 **several screen shots, and in response to those questions**
14 **you were saying, well, those documents in the screen**
15 **shot are being shared.**
16 **Do you mean that they were actively being**
17 **downloaded by someone else on the peer-to-peer network**
18 **at that particular time that the screen shot was taken?**
19 A. No, sir.
20 As I said during the portion where I described
21 how peer-to-peer networks work, sharing is different
22 than downloading. "Sharing" means the files were
23 available and could have been downloaded by anyone.
24 "Downloading" means that they would have been
25 downloaded.

892

The evidence I presented shows sharing. I have not been presented any evidence of downloading.

Q. So instead of saying the files are being shared, would it have been a correct statement to say that the files were made available for sharing?

A. I use the term "sharing" as being the -- defined as being available for downloading. If you would like to use the term "available" or "shared" as being available for downloading, I can work with that. But my definition is, if they were shared, they're available for download for anyone on the Gnutella network.

Q. Well, I just wanted to clear up for those of us who don't deal in this area every day that there is a difference when you say the files are being shared and whether or not someone is actually downloading the file.

And so I think you've cleared it up, that when you say that the file is being shared, you mean that it's available, it's made available for sharing and not necessarily being downloaded at that particular time.

A. Right. I'm happy to draw a distinction between a file being shared and being downloaded. Being shared does not mean it's downloaded.

Q. Did you try to find the 1718 File?

A. No, sir, I didn't.

893

Q. So before this case, how familiar were you with LimeWire, the program LimeWire itself?

A. Well, I have a very long experience in peer-to-peer protocols going back to graduate school in about 1995. I have experience --

Q. Can I stop you?

A. I'd prefer you didn't. May I answer the question?

Q. Go ahead.

A. I have experience with the Gnutella network pretty extensively through grants and through developing law enforcement tools that search the network.

LimeWire is just one example of a client that works on the Gnutella network. It does not differ appreciably from other clients.

So I have not a lot of experience with LimeWire directly, but it is similar to things that I have very extensive experience with.

Q. So the answer to my question is that you do not have a lot of experience with LimeWire directly; correct?

A. I have not had a lot of experience dealing with the particular LimeWire Gnutella client directly, no.

Q. In fact, in preparing to formulate your opinion, you studied the LimeWire source code; is that

894

correct?

A. Yes. That was part of what I did to prepare.

Q. In fact, as you were preparing to give your opinion, you studied the LimeWire design documents; is that correct?

A. Yes. In part.

Q. And in fact, you found those documents on the Wayback Machine; is that correct?

A. Yes, that's where I found those.

Q. You were asked about crawlers.

And I think you said that some of your students could create crawlers, it's not that difficult to do; is that correct?

A. Yes.

Q. And I guess the simplest crawler would not have the ability to download files from a peer-to-peer network or would it?

A. It depends on the type of crawler you're trying to build and the information you're trying to gather with the crawler.

Q. So outside of the academic realm, someone who would build a crawler, what purpose, I should ask then, would someone build a crawler or design a crawler?

A. I can -- the best way to answer that question is to say what the crawler's abilities are, and somebody

895

who is interested in taking advantage of those abilities would want to build one.

Q. What are the abilities of a crawler?

A. The crawler can perform a variety of functions. One of the things it can do is it can measure membership and find membership, that is, all the peers that are participating.

One of the things on Gnutella it can do is utilize the browse host extension to find the names of all the files that are being shared on the network. A particular crawler might also choose to download some of those files and process them for some purpose, but...

Q. In terms of downloading files or information from a peer-to-peer network, when you download a file, you have to keep it somewhere, don't you?

A. When you download a file, you're typically storing that file on your computer somewhere. Yes.

Q. And so if it's your practice to go out on a daily basis and crawl a peer-to-peer network and download files, let's say, four or five hours a day, would you have to have a large space to store all the files you could download off the peer-to-peer network, say, over the course of five hours a day?

A. No, sir, not necessarily. It would depend on

904

1 A. No, sir.
2 **Q. They're not?**
3 A. My conclusions are not hypothetical. My
4 conclusions are based on my years of experience, the
5 fact that this type of misconfiguration has been known
6 for a while and that they were warning against it. It's
7 based on a review of the evidence to determine what was
8 most likely.
9 **Q. So how was the LabMD file exposed, I mean,**
10 **actually shared? How was it shared?**
11 A. I don't know how it was actually shared. I
12 don't have the evidence. All I can say is, based on my
13 experience and what I reviewed, what the probabilities
14 are.
15 **Q. Okay. So were you given the information that**
16 **Tiversa and its CEO Mr. Boback has indicated that he**
17 **found the -- or Tiversa -- I don't know if he did**
18 **personally, but that he found the 1718 File, but he**
19 **didn't find it at LabMD?**
20 A. I don't recall the specifics of where they found
21 it.
22 **Q. So you weren't really given that information to**
23 **draw your conclusions from?**
24 A. No, sir. I believe it was in there. It just
25 didn't play a major part in my report, so I don't

905

1 actually recall.
2 **Q. So your focus was to come up with a likely**
3 **scenario as to how the file left LabMD's possession?**
4 **Was that your focus?**
5 A. I wouldn't phrase it in the terms of a likely
6 scenario. I would phrase it in the terms of what the
7 most likely scenario was given the evidence that we
8 had.
9 **Q. Given the events of what?**
10 A. The evidence that we had.
11 **Q. Okay. All right. Well, given the evidence that**
12 **you were exposed to.**
13 A. Yes, sir. That would be a better way of saying
14 it. Thank you.
15 **Q. Okay. CX 703.**
16 **At page 112.**
17 **Mr. Shields, I'm going to ask that you give no**
18 **emphasis to the shading, just ignore it. It doesn't**
19 **mean anything.**
20 A. Sure.
21 **Q. And if you could start at -- well, let me do**
22 **this.**
23 A. May I ask what this exhibit is? I didn't see
24 what it was.
25 **Q. This is the testimony of Mr. Robert Boback.**

906

1 **Did you review that in --**
2 A. I believe so. I just didn't see what was put up
3 on --
4 (Admonition from the court reporter.)
5 JUDGE CHAPPELL: Well, they can, but you just
6 can't -- we obviously know they can, they just did, but
7 she can't take it down, so let's go one at a time.
8 BY MR. SHERMAN:
9 **Q. Page 112 line 11:**
10 **"QUESTION: You would agree that there are a**
11 **variety of ways for information, such as the 1718 File,**
12 **to get on the Internet; correct?"**
13 **There's an objection interposed there.**
14 **"For example, someone could put a thumb drive**
15 **containing the file into a computer, and if that**
16 **computer had a peer-to-peer network downloaded into it,**
17 **it would be shareable, in other words, it would be**
18 **available to a company like yours" -- I'm talking about**
19 **Tiversa -- "or anyone else who would go and make the**
20 **appropriate search to find it; is that correct?**
21 **The answer: "Yeah, it could be, sure, that is**
22 **one plausible way."**
23 **Did you consider that when you arrived at your**
24 **conclusions here, that --**
25 A. Yes.

907

1 **Q. -- Mr. Boback, the CEO of Tiversa, said yeah,**
2 **well, it could have gotten on the Internet on a**
3 **peer-to-peer network, some other way other than being**
4 **shared by LabMD?**
5 A. I did read that as part of his deposition, yes.
6 **Q. And did you also know that Mr. Boback didn't**
7 **really know how the file got on the IP addresses where**
8 **he found them?**
9 A. Yes.
10 **Q. And so your task really was to come up with the**
11 **most likely scenario, based on the facts that you were**
12 **given, as to how the file escaped LabMD's possession.**
13 A. Yes.
14 **Q. And so since nobody really knows -- you would**
15 **agree that nobody really knows how it got out?**
16 A. Yeah. I -- I don't know what other people know,
17 so I don't want to say yes, but I don't know. How's
18 that?
19 **Q. Right.**
20 **And in your review of the record, you haven't**
21 **been able to find any evidence or testimony where**
22 **someone says, Hey, this is how it got out; correct?**
23 A. That's correct.
24 **Q. I've got a couple of questions about some of the**
25 **slides that you showed us and I'm just going to try and**

In the Matter of:

LabMD, Inc.

May 27, 2014
Trial - Public & Nonpublic Record
Volume 5

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION

I N D E X

IN RE LABMD, INC.

TRIAL VOLUME 5

PUBLIC AND NONPUBLIC RECORD

MAY 27, 2014

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
DAUGHERTY	936	1038	1096		
KAUFMAN	1100				

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
Number532	1116			
JX				
(none)				

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 27, 2014
9:34 a.m.
TRIAL VOLUME 5
PUBLIC AND NONPUBLIC RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
MARGARET LASSACK, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

942

1 clearly bothering them was that they were having
2 trouble with their laboratories because -- and I do --
3 if you could -- I'm going to step back a second and
4 explain this so that His Honor understands why this is
5 relevant, if I may.
6 In the late '80s, prostate biopsies were a
7 primarily -- that was the end of them being primarily a
8 hospital-based procedure because the technology had
9 advanced so that ultrasound machines could be mobile.
10 This created a situation where a urologist could
11 now, instead of taking his patients into the hospital to
12 have this procedure done, he could bring them into his
13 office. And that was less expense, less time in the
14 hospital. It was just better for everybody because it
15 wasn't really that huge a procedure.
16 This suddenly created the situation where the
17 doctor could actually choose who read his tissue. He
18 wasn't locked in to the hospital pathology team.
19 Now, with all due respect to pathology --
20 hospital pathology teams -- let me grab water here.
21 Excuse me -- those are generalists. And if you have
22 cancer, and the person diagnosing your cells is a
23 pathologist, logically you would like to have someone
24 that just reads that type of cell because practice
25 makes perfect and cancer isn't cancer. All sorts of

943

1 different types of cancers are different types of cells,
2 formations, genetics, everything.
3 So this whole industry was born so physicians
4 could send tissue elsewhere. And back then, the biggest
5 challenge was convincing a physician that putting
6 tissue in a Federal Express box and sending it across
7 country was okay.
8 But the benefit they got was pathologists that
9 just were practicing that niche of prostate cancer or
10 bladder cancer.
11 And so that was -- that really did quite well.
12 That happened in many aspects of medicine.
13 The problem then with the --
14 MS. VANDRUFF: Objection, Your Honor.
15 I'm not certain how this is responsive to
16 Mr. Sherman's question. And this is a narrative, and
17 I'd just ask that this be conducted as an examination.
18 MR. SHERMAN: I can break up the narrative with
19 questions if Your Honor would like.
20 The question was --
21 JUDGE CHAPPELL: I'm looking at it.
22 I don't see it as nonresponsive. It's a pretty
23 broad question.
24 However, if you could conduct in a more
25 question-and-answer routine, that would be better.

944

1 MS. VANDRUFF: Thank you, Your Honor.
2 MR. SHERMAN: Thank you, Your Honor.
3 JUDGE CHAPPELL: So the objection is sustained.
4 MR. SHERMAN: I'll direct the witness.
5 THE WITNESS: So am I not supposed to finish
6 that because I'm right --
7 BY MR. SHERMAN:
8 **Q. No. Let me ask you some questions.**
9 **You said that pathologists -- hospital**
10 **pathologists were generalists.**
11 **What did you mean by that?**
12 A. That means that they would read lots of
13 different type of cancers. And there's only so much
14 time in the day, so many of them -- most of them are not
15 expert in prostate.
16 **Q. Okay. And so part of your idea was to do what?**
17 A. Part of my idea was to solve the next problem,
18 which I was just about to say, which is, there became a
19 secondary problem with that because managed care
20 exploded in the '90s, and suddenly these physicians had
21 all these specimens in their office, and they were being
22 told where they had to go based on a managed care
23 contract.
24 And instead of the tissue being in the
25 hospital, now the tissue is in the office. And at the

945

1 end of the day, you have a nurse that's got twenty
2 tubes of blood, ten tubes of urine, two to three
3 biopsies, and she now has to send them to each
4 laboratory. And if she --
5 **Q. Now, how was it determined which laboratory the**
6 **samples would be sent to?**
7 A. The office staff would have to compile a list
8 and at times call insurance proactively to find out
9 what laboratory their insurance carrier required if
10 there was a requirement. And if they didn't do that,
11 then the insurance carrier was going to deny the claim
12 or reduce the benefit, the patient is going to get a big
13 bill, and the patient is going to be very mad at the
14 physician.
15 So what happened was you had these back,
16 you know, clinical areas of offices that had lists taped
17 on cupboard doors and staff that would have to call if
18 there was insurance policy that wasn't on there so that
19 they would know where to -- so they were having to just
20 organize all of it.
21 **Q. Are you talking about doctors' offices and their**
22 **staff having to organize this?**
23 A. Yes, I am.
24 **Q. And how did you set out to help or resolve that**
25 **problem?**

954

1 MS. VANDRUFF: Objection, Your Honor. To the
2 extent that Mr. Sherman is calling for fact testimony, I
3 believe that may be permissible, but I think this walks
4 a fine line of opinion testimony.
5 JUDGE CHAPPELL: Is this disputed?
6 MS. VANDRUFF: I'm sorry, Your Honor?
7 JUDGE CHAPPELL: Are you saying, what he just
8 asked, this information is disputed by the government?
9 MS. VANDRUFF: I'm not certain exactly what he
10 is eliciting. I think he is to compare what the
11 services LabMD offered to what services other companies
12 offered. It's not a material fact in this case,
13 Your Honor.
14 JUDGE CHAPPELL: Based on what I've heard, the
15 witness knows enough to answer the question.
16 Overruled.
17 MS. VANDRUFF: Thank you, Your Honor.
18 THE WITNESS: It's easier to draw it, sir, if I
19 can draw it.
20 BY MR. SHERMAN:
21 **Q. You might want to pull the easel out so -- I**
22 **think the court wants everyone to be able to see it.**
23 **(Pause in the proceedings.)**
24 **So, Mr. Daugherty, if you could, define or**
25 **sketch out the process that you thought was the**

955

1 **problem, and after doing so, kind of scale or draw out**
2 **the process that you believe was the solution.**
3 A. Okay. Prior, the receptionist in a urologist's
4 office would have to give the -- by handwritten
5 information --
6 (Discussion off the record initiated by the
7 court reporter.)
8 THE WITNESS: Everything before is manual. The
9 receptionist --
10 (Discussion off the record initiated by the
11 court reporter.)
12 JUDGE CHAPPELL: Does he really need the chart?
13 I can understand what he's saying without the chart.
14 That will make it simpler.
15 MR. SHERMAN: That's fine, Your Honor. It kind
16 of helps him, but we'll push through.
17 (Pause in the proceedings.)
18 BY MR. SHERMAN:
19 **Q. So, Mr. Daugherty, you were saying that in the**
20 **process, everything was done by hand.**
21 A. The -- the receptionist has to hand the
22 information to the nurse. The nurse has to pull the
23 information from the chart. Then she has to manually
24 fill out the form.
25 Or if they have one lab, they have to type it

956

1 into a workstation. They still have to fill out the
2 form, put it on the specimen, hold that copy for them to
3 make sure the -- the requisition, they'd hold a copy of
4 the requisition for them, they'd hold a copy of the
5 requisition in the patient chart, and they'd put a copy
6 of the requisition with the lab.
7 And they have to have a central chart, a central
8 record of what specimen went where.
9 **Q. And in filling out the record --**
10 A. The requisition.
11 **Q. -- the requisition that they would keep for**
12 **themselves, keep for the patient chart and then send to**
13 **LabMD, they would fill that out by hand as well?**
14 A. Correct.
15 **Q. And after, after they fill out the requisition,**
16 **what would happen?**
17 A. Okay. Then a courier would pick the specimen
18 up. The laboratory would have to manually enter the
19 information into their system for whatever lab was
20 there.
21 **Q. Once they received the specimen and the**
22 **requisition?**
23 A. There was one requisition with the specimen
24 that would arrive with whatever laboratory the doctor
25 chose to use for that specimen. And that staff in that

957

1 laboratory would have to start that process over of
2 entering the data into their system.
3 And then, depending on the lab, that type of --
4 that chain of custody through the process of the lab
5 would -- it grew into some barcoded issues, but that was
6 still very early where things were written. And then
7 the -- and then when the result is finished, a
8 transcriptionist would have to enter everything into the
9 laboratory's information system.
10 Then that would have to be approved by the
11 physician, the pathologist that works inside the
12 laboratory, and then that result would be released and
13 printed off.
14 At that point, it was a client preference in
15 the industry that the result would either be faxed to
16 the physician's office, which, quite frankly, wasn't
17 that legible, or sent Federal Express or mailed.
18 And every step along the way had issues that we
19 tried to eliminate from incorrect diagnoses codes that
20 would make you have to call them back to can't read
21 things to missing information to FedEx getting caught in
22 a storm.
23 **Q. So when you say incorrectly inputted diagnosis**
24 **codes that would make you have to call them back, are**
25 **you saying that these requisitions would arrive at the**

958

1 **lab, there was -- from time to time there would be an**
2 **incorrect diagnosis code, the staff of the lab would**
3 **then have to call back to the doctor's office and get**
4 **the correct diagnosis code?**
5 A. Correct.
6 And it was more -- Medicare required that if a
7 test was being performed on a patient with a diagnosis
8 the physician had given that was not approved by
9 Medicare for payment, the doctor would have to pay that
10 bill unless -- unless he notified the patient and the
11 patient signed off that it was okay. Just that alone
12 could kill the specimen stability time.
13 So you've got a day later usually the specimen
14 arrives. You have to chase down a nurse, who's going to
15 be way less than happy that she's made an error, and
16 then she would chase a doctor and then -- and usually it
17 was just the fact that they made an error that everyone
18 knew in urology, you know, what usually would be
19 covered.
20 **Q. Do some specimens have a shelf life that --**
21 A. Yes. They almost all have shelf lives, and it
22 varies, I mean, from CBC with diff can be two to four
23 hours and CBC without diff can be 24 hours.
24 **Q. And so the type of mistake that you just said**
25 **could affect the shelf life of a specimen and maybe**

959

1 **require the patient to come back and get another one.**
2 A. Correct. And then you have to restick the
3 patient and -- so the potentials were numerous, and it
4 became a large -- well, it was a large bureaucratic
5 problem because when you have to deal with five labs
6 instead of one, it's just it added -- it just compounded
7 the issues.
8 **Q. So what process did you put in place?**
9 A. Okay. So I took an existing laboratory
10 information system and -- and the idea was to just
11 streamline the process by hiring people to put
12 additional features and benefits in the software so
13 that what we did was we would go into a account, a
14 physician's office. We would get their entire
15 insurance database, and we would give it a primary
16 additional code so that we would know, for example,
17 that Blue Cross HMO from that state for that doctor
18 would have to go to LabCorp versus Blue Cross HMO from
19 another state for a client in Arizona would have to go
20 to Quest.
21 If all that was programmed in the system ahead
22 of time, what happened was, the second the nurse placed
23 the order, the -- and I'm jumping over something I have
24 to go back to -- but the second the nurse placed the
25 order, we had the database populated with all the

960

1 patients that were in the physician's office, so that
2 saved all this time.
3 And the doctor didn't know who he was going to
4 place an order on that day. But everything was in the
5 database so that it could look and see, well, that has
6 to go to LabCorp, this has to go to Quest. And they
7 don't have to worry about it anymore, so all those
8 papers went away.
9 And then also the software would go, okay, you
10 just tried to place an order with a nonpayable code.
11 The computer won't place the order. Nurse, you must
12 stop and make your correction or you have to print off
13 the disclosure form for your physician and patient to
14 sign.
15 This is proactivity to increase patient result
16 speed because people want to know if they do or don't
17 have cancer as soon as possible, reduce any pitfalls of
18 error. It's just a win-win everywhere.
19 **Q. And so I think we're at the first stage here --**
20 A. Okay.
21 **Q. -- where the nurse --**
22 A. The first stage is when -- because we're -- the
23 less -- the less data entry you have, the less error
24 you have.
25 So by having the receptionist in the

961

1 urologist's office put the data from the urologist's
2 office in their system, which they're going to do
3 anyway because they're getting paid for services as
4 well, for the visit, et cetera, and the procedure, that
5 would be sent over to the -- to LabMD technologically.
6 And that would be sent over, and then it would
7 be there ahead of time for -- in the lab database. And
8 then -- and it -- and when it came over was dependent on
9 the physician's office because this is very early
10 adapter, very ahead of time, and everyone had different
11 software and all of this software is dependent on how
12 they did it, how we got it.
13 By and large, that was what happened.
14 Then, whether it be 30 minutes or at the end of
15 the day or the next day, depending on the specimen, the
16 data would be in there. The nurse could just pull up
17 the patient and everything is populated. Everything is
18 there (indicating).
19 And it's legible and it's clear, and if there's
20 missing fields, you're prompted to fill them up. And
21 when you put a diagnosis code in, it's going to tell
22 you if it's payable and correct or if you're going to
23 have to work with the patient and you can't move on.
24 And then a barcode would come off, and then the
25 specimen is barcoded with identifiers that are legible

962

1 and clean and almost always correct. And then that
2 saved time.
3 And then also at the end of the day, the staff
4 would print off everything that they had ordered. And
5 it would give a list and it would say what lab it went
6 to.
7 And in our marketplace, typically approximately
8 85 percent of all the specimens were allowed to come to
9 LabMD. But that 15 percent that weren't allowed to
10 come to LabMD, by removing all the pitfalls of having to
11 manage that was a huge time savings and a huge removal
12 of bureaucracy from physicians' offices.
13 Then when the specimen got to the laboratory,
14 everything also was -- I mean, the amount of errors just
15 fell through the floor. The time that they got
16 processed went quicker. And the -- the -- we even knew
17 ahead of time what was coming so that we could be
18 prepared.
19 **Q. So when the nurse at the physician's office**
20 **would enter the -- well, put in the requisition for a**
21 **test, that information would be communicated**
22 **immediately to LabMD when the requisition was**
23 **completed?**
24 A. When the -- when the button -- when the "send"
25 button or "order" button was pressed, that immediately

963

1 electronically was sent to LabMD.
2 **Q. And upon receipt of that information, you were**
3 **indicating that LabMD could then be prepared?**
4 A. Well, before then you wouldn't know what was
5 going to come until it showed up. I mean, you just
6 didn't know, so you didn't know if anything was missing
7 either.
8 But we had -- we knew ahead of time so we could
9 know what was supposed to be coming. We could prep. We
10 could have the proper staffing. We could have the
11 cartridges ready ahead of time. We could have
12 everything ready, which also sped things up, also
13 increased accuracy.
14 We also then knew if something didn't arrive
15 that should have. And that was new. It was like we
16 were expecting it. That actually created a lot of
17 issues, because if the nurse just threw it in the
18 refrigerator and forgot, where is it, we got it, no
19 worry.
20 **Q. So by being able to anticipate what samples are**
21 **coming to the lab, what could you do ahead of time which**
22 **would affect a quicker test result?**
23 A. Prep the slides, have the proper staffing, let
24 the physician know what his day is going to look like,
25 prioritize what's coming in, know what's coming in from

964

1 which part of the country and, I mean, the list goes on
2 and just -- and then also have the ability to do an
3 inventory at the beginning of the day when the specimens
4 do arrive to see if anyone screwed up and something
5 didn't show up.
6 **Q. So you know what's coming. You have the staff**
7 **prepared for the next day's samples. They do their job.**
8 **Then how -- how are the test results then -- how**
9 **are the test results then gotten or --**
10 A. Received by the physician; is that what you
11 mean?
12 **Q. No. No.**
13 A. Oh, gotten by --
14 **Q. How do you do what you do in order to get the**
15 **test result?**
16 A. Oh, okay.
17 Depending on the test, only the physician or a
18 physician-supervised technologist can release test
19 results. That's not anything that anyone like I or an
20 officer of the company could do. And so -- yeah?
21 **Q. Would the photographs kind of help walk us**
22 **through this process?**
23 A. Yes.
24 **Q. Okay.**
25 A. Sorry.

965

1 **Q. So let's show the outside of LabMD.**
2 A. Okay.
3 **Q. So what is that a picture of?**
4 A. Okay. This is the entrance to the LabMD
5 facility that was there from 2008 -- April 2008 to when
6 we closed.
7 **Q. Either speak up or pull that closer to you.**
8 A. Okay. Sorry.
9 So this is the accessioning entrance to LabMD at
10 our location where we were operating from.
11 **Q. What happens at that particular entrance?**
12 A. That is the accessioning entrance where either
13 Federal Express -- no. I'm sorry -- our courier or
14 employee brings the specimens in. We would go to
15 Federal Express and get them.
16 **Q. You used the term "accessioning" and I -- I'm**
17 **sorry. I don't know what that means.**
18 A. Accessioning is the organizing and accepting of
19 the specimens into the laboratory and the distribution
20 to the appropriate testing department.
21 **Q. Okay.**
22 A. So this is typically how each specimen would
23 arrive. It was ironic that we didn't really need
24 requisitions and paper, but the physicians just
25 couldn't let go of it, so -- so we turned it into our

1018

1 A. Yeah. It would have been easier to have them
2 all unredacted, so we thought that would be forthcoming
3 and that was no big deal, so -- but we only had 60 days
4 per the regulation, so -- but we thought it would be
5 forthcoming, so we didn't take the long road until they
6 just didn't come. And then I -- I just directed my --
7 my lawyer to just figure out through our staff how we
8 can connect these billing transaction codes to
9 patients.
10 **Q. How did you connect the billing transaction**
11 **codes to patients?**
12 A. We had to go to Lytec and pull each one up one
13 by one and see what patients could be possibly attached
14 to that transaction number.
15 **Q. So what is Lytec?**
16 A. Lytec is the software that we use in the billing
17 department, and that is the software that generated this
18 report.
19 **Q. And what did you enter into Lytec to try to find**
20 **out what the full patient information --**
21 A. This billing number, this billing number that's
22 on the sheet that's to the left of the -- what looks
23 like the date.
24 **Q. And so --**
25 A. It says "Billing" in the heading.

1019

1 **Q. And so it's fair to say that by using the**
2 **billing number you were able to discern who, whose names**
3 **appeared on the day sheets; correct?**
4 A. Well, we were to reasonably assume since we
5 didn't see it, so my recollection is that what we
6 received was way more redacted than this, that there was
7 nothing open except like the heading and that one
8 column.
9 **Q. And which column?**
10 A. The Billing column, the column that says
11 "Billing," that one --
12 **Q. But using that information you were able to**
13 **discern --**
14 A. That's correct, we were able to discern.
15 **Q. -- the names of the people who were on the day**
16 **sheets.**
17 A. Yes. Who they likely were, yes, who's attached,
18 correct.
19 **Q. Mr. Daugherty, up on the screen is RX 348.**
20 **Do you recognize that document?**
21 A. That's the notification letter we sent to the
22 patients that we put together were on the day sheets.
23 **Q. And what's the date of that letter?**
24 A. March 27, 2013.
25 **Q. And why did you send this letter?**

1020

1 A. Well, HIPAA requires, after the rule went in
2 effect and -- and out of a abundance of caution -- the
3 last day sheet was dated prior to that notification rule
4 going in effect in 2009, but out of an abundance of
5 caution, we didn't want to go round and round on when
6 these were taken.
7 We thought these were taken right in line with
8 our move because that's right when we were packing up
9 and moving when the last one was -- was -- was -- the
10 last day sheet was -- was -- the old -- I guess the
11 youngest day sheet they'd call it. You know, the
12 day sheet dates were from 2000 to 2009, so we just
13 assumed -- we assumed, okay, we're really a small group
14 here. These are not burned on the hard drives. This
15 is not about any firewall or any -- anything
16 electronic. This is a physical paper document theft if
17 that. We don't have the information, but what do we
18 know that would let us, you know, know when this
19 occurred.
20 At the same time, we weren't getting answers
21 from the Federal Trade Commission, and we were
22 concerned about HIPAA. We really felt like that we had
23 to honor HIPAA, especially because we felt like the FTC
24 was setting us up to fail.
25 So out of an abundance of caution, we pretended

1021

1 that this happened the day that we were told by the FTC,
2 even though we found out it had happened almost four
3 months before.
4 **Q. What --**
5 A. Okay. So -- so anyway, so we sent this to
6 patients because HIPAA required it.
7 **Q. And you sent it on March 27, 2013; correct?**
8 A. Correct.
9 **Q. And it's your testimony that you learned that**
10 **the FTC was in possession of these around the end of**
11 **January; is that correct?**
12 A. Correct. So we had 60 days.
13 **Q. Okay. Did you find out when the FTC came into**
14 **possession of the day sheets?**
15 A. Yes.
16 **Q. And when did the FTC come into possession of the**
17 **day sheets?**
18 A. Well, they became aware of them in mid-October
19 of '13, and they became in possession shortly thereafter
20 in October 2013 from the Sacramento police, according to
21 what the Sacramento police told us.
22 **Q. So it's your testimony that the FTC became aware**
23 **in mid-October and that they did not notify LabMD until**
24 **late January?**
25 A. That's correct.

1026

1 identity theft.
2 And I would need to review the transcript of the
3 witness to determine with certainty what she said
4 specifically about the LabMD documents that were found
5 in their possession. I believe she said that she did
6 not know.
7 MR. SHERMAN: Well, Your Honor, the exhibit
8 that I'm attempting to proffer or bring into the
9 court's current view and knowledge is an e-mail from
10 Detective Jestes to Mr. Sheer and Ms. Yodaiken
11 concerning just that issue as to whether or not the
12 day sheets in fact and the receipt of the day sheets in
13 fact have anything to do with the two individuals who
14 pled.
15 MS. VANDRUFF: And Your Honor, this document is
16 in the record, and so to the extent that the court
17 wishes to draw inferences from it or from the testimony
18 of the witnesses who have been examined, that certainly
19 is within the province of the court, but I don't
20 believe it's a proper subject of Mr. Daugherty's
21 examination.
22 JUDGE CHAPPELL: We have an improper foundation
23 for it to be utilized with this witness at this time.
24 Sustained.
25 MS. VANDRUFF: Thank you, Your Honor.

1027

1 BY MR. SHERMAN:
2 **Q. So, Mr. Daugherty, you now learned that the case**
3 **is about the 1718 File and the day sheets as late as**
4 **January of 2013; correct?**
5 A. Correct.
6 **Q. And is it your position that at that point you**
7 **still don't know what you did wrong?**
8 A. That's correct.
9 **Q. And Mr. Daugherty, what impact -- and I would**
10 **say as the investigation proceeded, what impact, if any,**
11 **did this have on your business?**
12 A. Well, it had -- it was -- it started out -- the
13 whole impact on the business started in May 2008 with
14 the beginning of a constant series of "we're not telling
15 you" from Tiversa and then the Federal Trade Commission.
16 And so it had --
17 **Q. What is it that you contend that the**
18 **Federal Trade Commission didn't tell you?**
19 A. They didn't tell us they had the day sheets for
20 three and a half months, even though we're subject to
21 HIPAA, which requires us to notify in 60 days. That
22 trust didn't need to be any further obliterated, but
23 that was validating at that point.
24 On the one hand we're supposed to protect
25 patients and we're supposed to follow the law, and yet

1028

1 the federal government is withholding information from
2 us, so it seems to me they're more eager to lambaste us
3 and entrap us than keep patients safe.
4 So we were outraged, scared, felt entrapped, and
5 employees were starting to really break under pressure
6 when that went down.
7 **Q. What other impacts did it have on LabMD's**
8 **business?**
9 A. It completely sideswiped, just the relentless
10 ghost of the FTC hovering over the company all those
11 years, because they continually showed up and wanted
12 more and wanted more and wanted more, and it -- look, I
13 have myself and a VP of operations and general manager.
14 I had three to four IT people. We were diagnosing
15 cancer and trying to run a medical facility, and we
16 can't get an answer about what we're supposed to do.
17 And we're being treated like we don't care or we're --
18 and what we're getting is brushstrokes of consent
19 decrees and we're getting, you know, read -- read this
20 information, and there's no straight answer. And this
21 is really -- I can't understate how damaging and
22 confusing and sideswiping this was to the attention,
23 energy and morale of the management staff that knew
24 because we, you know, had a company to run.
25 We had Obamacare coming. We had to diversify

1029

1 our base, and we were -- and we're being financially and
2 attention -- I guess attention energy, I guess planning
3 energy, goal energy, management's energy being diverted
4 by this looming what-if.
5 So this -- go ahead. I --
6 **Q. Was there any impact -- I take it what you just**
7 **said described the impact on the business internally.**
8 A. Uh-huh.
9 **Q. Was there any impact on the business**
10 **externally?**
11 A. Yes.
12 **Q. And what was that?**
13 A. Well, the press broke the story in 2012, so once
14 the press broke the story, I had -- you know, you can't
15 control perception, and so I had physicians upset with
16 me they didn't hear it from myself. I had people
17 concerned that I -- I mean, there was again -- I guess
18 the cloud of suspicion just got greater, because
19 evidently in this process you're guilty until proven
20 innocent, and so people were just assuming, well,
21 there's something going on at LabMD or what's going
22 on -- and when you're trying to plan to grow, that is a
23 hard thing to have to deal with.
24 So I was at a Christmas party for one client,
25 and you know, she was a physician who was upset with me

1030

1 she had to learn about it from the newspaper.
2 And those kind of things, I don't know how much
3 else went on behind my back.
4 I did find out later, for example, the rumor had
5 twisted around so that -- because, you know, most people
6 in medicine don't know what the FTC is, so I'm getting
7 told, I hear you're in trouble with the SEC about some
8 trade -- I mean, just the rumors just went crazy.
9 **Q. Did you lose clients as a result of the impact**
10 **of this investigation and litigation?**
11 A. Okay. See, it's not black-and-white losing
12 clients because you lose pieces of clients.
13 So we had some clients -- they were so in --
14 like that one account, they sent us less stuff except
15 for what was really beneficial with the software, so I
16 think the impact was much greater in the growth than in
17 the actual loss of clients. But then the clients
18 themselves -- we had one client who -- the person that
19 had said they wished they had learned it earlier, there
20 was no growth there and they did use other labs for a
21 few other things.
22 **Q. Did the investigation process have an impact on**
23 **your third-party providers?**
24 A. Well, once we were sued, the Federal Trade
25 Commission carpet-bombed with approximately forty

1031

1 subpoenas to physicians and third-party vendors and
2 employees that had been with the company for years, and
3 that of course again just stirs the psychological
4 warfare pot, and there's just one of me, so yes, that
5 had a negative effect.
6 **Q. Mr. Daugherty, what is the current state of**
7 **LabMD's operations?**
8 A. LabMD is in a very deep coma. We are still in
9 business. The corporation is still standing. I'm the
10 only employee.
11 All we do -- we preserve the slides and the
12 electronic data for the physicians so they can still get
13 results if they don't have them and they can still send
14 slides out for second opinions.
15 Because that goes on, you know, that doesn't
16 just stop. Those are -- patients can have -- prostate
17 cancer is a very slow-growing disease, so you can have
18 it for 14 years, so -- and there's technologies that
19 kept -- are available now to analyze versus what was
20 available five years ago on -- on aggressiveness of the
21 tumor cells, so we keep all that available still.
22 And then we also still have accounts receivable
23 that we still have to try to work from last year.
24 But other than that, we're being sued by the
25 landlord for early termination for between 800 and

1032

1 900 thousand dollars.
2 We have consolidated everything into the
3 corporate condo, and I don't want to say on the public
4 record actually where else things are if this is public,
5 so...
6 **Q. What's the state of LabMD's insurance coverage?**
7 A. Well, in the beginning, we of course had medical
8 insurance, dental insurance, workmen's comp, vision,
9 general liability, medical malpractice for the
10 physicians, medical malpractice for the facility.
11 So of course we had to let everybody go. They
12 still have dental and medical through COBRA should they
13 choose at their expense. The vision is gone. The
14 workmen's comp is gone. The -- before -- the general
15 liability for the corporation has been nonrenewed
16 because of the Federal Trade Commission action and
17 claims.
18 The --
19 **Q. How do you know that's the reason?**
20 A. Because they told us.
21 The medical malpractice -- when you close --
22 obviously we're not practicing medicine now and moving
23 forward, so the medical malpractice is for tail coverage
24 for any claims -- any claims from any practiced medicine
25 we did in the last few years would be covered in the

1033

1 future for the next couple of years.
2 We had carriers that flat-out would deny to
3 quote us because of the Federal Trade Commission
4 investigation, even though, you know, these are medical
5 malpractice. I don't think that the
6 Federal Trade Commission has any jurisdiction over
7 medical malpractice. I don't know, so -- but they
8 didn't care.
9 And then we had a -- we got -- I got tail
10 coverage for the physicians, and there were many fewer
11 insurance carriers that were willing to quote it. But
12 we did get insurance for -- we did get tail coverage for
13 the two physicians that we had to let go.
14 MR. SHERMAN: One moment, Your Honor.
15 JUDGE CHAPPELL: Okay.
16 (Pause in the proceedings.)
17 MR. SHERMAN: I have no further questions,
18 Your Honor.
19 JUDGE CHAPPELL: I have a few.
20 THE WITNESS: Yes, sir.
21 JUDGE CHAPPELL: Sir, I'm not asking you to
22 speculate in any way. I just want you to tell me what
23 you know.
24 THE WITNESS: Okay.
25 JUDGE CHAPPELL: If this cloud that you refer to

In the Matter of:

LabMD, Inc.

May 30, 2014
Trial - Public & In Camera Record
Volume 7

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION

I N D E X

IN RE LABMD, INC.

TRIAL VOLUME 7

PUBLIC AND IN CAMERA RECORD

MAY 30, 2014

WITNESS: DIRECT CROSS REDIRECT RECROSS VOIR
(none)

EXHIBITS FOR ID IN EVID IN CAMERA STRICKEN/REJECTED
CX
(none)

RX
(none)

JX
Number3 1242

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 30, 2014
9:35 a.m.
TRIAL VOLUME 7
PUBLIC AND IN CAMERA RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
MARGARET LASSACK, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
MICHAEL PEPSON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

ON BEHALF OF RICK WALLACE:
WILLIAM A. BURCK, ESQ.
LAUREN DICKIE, ESQ.
Quinn Emanuel Urgquhart & Sullivan, LLP
777 6th Street, N.W.
Eleventh Floor
Washington, D.C. 20001-3706
(202) 538-8000
williamburck@quinnemanuel.com

CONFIDENTIAL — REDACTED IN ENTIRETY

In the Matter of:

LabMD, Inc.

May 5, 2015
Trial - Public & Nonpublic Record
Volume 9

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

FEDERAL TRADE COMMISSION
I N D E X
IN THE MATTER OF LABMD, INC.
TRIAL VOLUME 9
PUBLIC AND NONPUBLIC RECORD
MAY 5, 2015

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
WALLACE	1337	1414			
		1421	1431		

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
Number545	1419			
Number546	1426			
Number549	1423			
JX				
(none)				

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of)
)
LabMD, Inc., a corporation,) Docket No. 9357
)
Respondent.)
----------)

May 5, 2015
10:11 a.m.
TRIAL VOLUME 9
PUBLIC AND NONPUBLIC RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
JARAD BROWN, ESQ.
ALAIN SHEER, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
PATRICK MASSARI, ESQ.
PRASHANT KHETAN, ESQ.
ERICA MARSHALL, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-4231
patrick.massari@causeofaction.org

ON BEHALF OF RICHARD WALLACE:
MARY BETH BUCHANAN, ESQ.
JACQUELYN N. SCHELL, ESQ.
Bryan Cave LLP
1290 Avenue of the Americas
New York, New York 10104-3300
(212) 541-1074
mbuchanan@bryancave.com

1377

1 this IP address resolves to Chicago and it's a complete
2 separate, you know, different computer.
3 JUDGE CHAPPELL: I'm just trying to clarify
4 this.
5 THE WITNESS: Uh-huh.
6 JUDGE CHAPPELL: If I understood you correctly,
7 it was not true that the file was at this IP address.
8 THE WITNESS: That is correct.
9 JUDGE CHAPPELL: And if I were Company B in my
10 earlier scenario, do I have any way to go to
11 Apache Junction and see if they've downloaded my data?
12 THE WITNESS: We would see that in our -- in our
13 real data store, we would show -- like, for example,
14 with this one, this individual had over -- I was very
15 familiar with this guy. He had over 3,000 tax returns,
16 and he was zipping them up and selling them. Therefore,
17 we knew that he was a bad actor, and it made it easy to
18 put this file there, so to speak, even though he never
19 had it physically on that computer, but we made it
20 look -- appear like he did.
21 JUDGE CHAPPELL: All right. So if I follow you
22 correctly, you never -- the file was never actually at
23 Apache Junction.
24 THE WITNESS: No.
25 JUDGE CHAPPELL: But I, Company B, had no way of

1378

1 ever verifying that or knowing that.
2 THE WITNESS: Right.
3 BY MR. SHERMAN:
4 **Q. For the other three IP addresses and line of**
5 **information on this document the same is true as for the**
6 **first line, that you put this information into Tiversa's**
7 **data store under these IP addresses for the purpose of**
8 **making it appear that the insurance aging file was found**
9 **there.**
10 A. That is correct.
11 MS. VANDRUFF: Objection, Your Honor. Leading.
12 JUDGE CHAPPELL: That's sustained.
13 I'll disregard the response to that question.
14 Do you want to rephrase?
15 MS. VANDRUFF: Thank you, Your Honor.
16 MR. SHERMAN: Yes, sir. We'll move through it.
17 BY MR. SHERMAN:
18 **Q. Line 2 on CX 19?**
19 A. Uh-huh.
20 **Q. What does the first set of numbers represent?**
21 A. That is an IP address.
22 **Q. The second set of numbers?**
23 A. Pardon me?
24 **Q. I'm sorry.**
25 **The second set of numbers, what does that**

1379

1 **represent?**
2 A. I still didn't hear you.
3 **Q. What does the second set of numbers --**
4 A. Oh, second set.
5 **Q. -- represent?**
6 A. That is the date, the date and time of the
7 modification or download.
8 **Q. And then the third line of information, the**
9 **third?**
10 A. That would be the file title as it would appear
11 in the data store for any input.
12 **Q. And is it true that you, Rick Wallace, went into**
13 **Tiversa's data store and entered this information under**
14 **the 68.107.85.250 IP address to make it appear that that**
15 **file was found there?**
16 MS. VANDRUFF: Objection, Your Honor. Leading.
17 JUDGE CHAPPELL: Yes. Beginning with "is it
18 true" pretty much indicates it's leading.
19 Sustained.
20 MS. VANDRUFF: Thank you, Your Honor.
21 BY MR. SHERMAN:
22 **Q. So the information that appears on the second**
23 **line?**
24 A. Pardon?
25 **Q. The information that appears on the second line**

1380

1 **of this exhibit?**
2 A. Okay. Yes.
3 **Q. You're familiar with that information; correct?**
4 A. Yes.
5 **Q. Did you place that information in Tiversa's data**
6 **store?**
7 A. Yes.
8 **Q. And why did you place that particular**
9 **information in Tiversa's data store?**
10 A. Again, this was after Bob came to me and said
11 that we needed a new spread on the insurance aging file
12 because there were some things going on between LabMD
13 and Tiversa and in no way, shape or form could it ever
14 have been found in Atlanta. There's something to do
15 with Bob claiming that we never connected to an IP -- to
16 a LabMD computer.
17 **Q. And is that true, that Tiversa never connected**
18 **to a LabMD computer?**
19 A. That is not true.
20 **Q. The third line of information on CX 19?**
21 A. Yes.
22 **Q. Oh, by the way, was the insurance aging file**
23 **ever found, to your knowledge, at 68.107.85.250?**
24 A. No, it was not.
25 **Q. The third line of information on CX 19, are you**

1381

1 **familiar with that information?**
2 A. That is also a known person who -- called an
3 information concentrator or an identity thief, someone
4 who is downloading information that's out there in the
5 wild that's available.
6 **Q. And did you place this information in Tiversa's**
7 **data store?**
8 A. Yes.
9 **Q. And the purpose of placing this information in**
10 **Tiversa's data store was for what?**
11 A. Because Bob had came to me, explained that we
12 had to have spread on these files and had to move it off
13 of the IP address that would emanate from and, you know,
14 in Atlanta.
15 **Q. And so that's what you did; correct?**
16 A. Yes.
17 **Q. The fourth line of information, are you familiar**
18 **with that as well?**
19 A. Yes.
20 **Q. And did you place this information in Tiversa's**
21 **data store?**
22 A. Yes.
23 **Q. And why did you place this information in**
24 **Tiversa's data store?**
25 A. It was just another IP address that was

1382

1 available that you could see was a bad actor.
2 **Q. If someone then goes into Tiversa's data store**
3 **and they see this information, what are they led to**
4 **believe?**
5 A. That the file was -- that the file would have
6 emanated from that IP address. It would -- it would
7 show up in a way, if you search for that IP address,
8 where it would be a laundry list of files and insurance
9 aging would show up in that list based on an IP search.
10 **Q. If you do an IP search of what?**
11 A. Of the data store.
12 **Q. Tiversa's data store?**
13 A. Yes.
14 JUDGE CHAPPELL: Who has access to the data
15 store?
16 THE WITNESS: Pardon me?
17 JUDGE CHAPPELL: Who has access to the data
18 store?
19 THE WITNESS: Basically every employee at
20 Tiversa.
21 JUDGE CHAPPELL: Did LabMD have access to the
22 Tiversa data store?
23 THE WITNESS: Did who? LabMD? No. No. We
24 would --
25 JUDGE CHAPPELL: I'm sorry. Let me restate

1383

1 that.
2 Was there a LabMD data store?
3 THE WITNESS: Was there?
4 JUDGE CHAPPELL: A LabMD data store.
5 MR. SHERMAN: May I, Your Honor?
6 THE WITNESS: I'm not sure --
7 JUDGE CHAPPELL: Go ahead.
8 BY MR. SHERMAN:
9 **Q. The question was: Was there a LabMD data**
10 **store?**
11 A. No. LabMD's data, I believe that there were
12 19 files total. They were all put in their own
13 directory on the data store along with millions of other
14 IP addresses.
15 JUDGE CHAPPELL: And these -- what is this
16 document number on the screen?
17 MR. SHERMAN: CX 19.
18 JUDGE CHAPPELL: CX 19, these four IP addresses
19 were created by you, and they're actually -- for all
20 practical purposes, they're fake, as far as the aging
21 file was not found on these three IP addresses;
22 correct?
23 THE WITNESS: On all four of them.
24 JUDGE CHAPPELL: And you created all four of
25 these at whose request?

1384

1 THE WITNESS: At Bob's.
2 JUDGE CHAPPELL: Bob Boback requested that.
3 THE WITNESS: Yes.
4 JUDGE CHAPPELL: How was this information
5 presented to LabMD?
6 THE WITNESS: It never was presented in --
7 other than I typed it up and I think it was either
8 e-mailed or -- I'm not really sure. But I know that
9 the actual file was never -- the actual files that were
10 doctored up were never provided to LabMD. They just --
11 I just had to put them in the data store so they would
12 look real.
13 JUDGE CHAPPELL: But again, if LabMD couldn't
14 access the data store, what was the point?
15 THE WITNESS: Because if there was ever an
16 audit or if somebody were to come in and say, Hey,
17 you know, show me a bad guy at 173, here he has already
18 been prosecuted by law enforcement and we know the IP is
19 dead, I would be able to show, wow, look at this. It
20 was basically for the wow factor.
21 One thing I would like to mention is the date
22 and the time was also adjusted on each file, so it was
23 very difficult at times and time-consuming because I had
24 to go backwards, like on the 11-5-2008 at 11:26 p.m.,
25 that file, the modified date on that had to be changed

1385

1 to reflect the same time frame when actual downloads
2 were happening from that IP address.
3 JUDGE CHAPPELL: Go ahead.
4 BY MR. SHERMAN:
5 **Q. You mentioned the word "spread."**
6 A. Uh-huh.
7 **Q. What does that mean?**
8 A. That would be where a file is available and it
9 appears to have been downloaded and being reshared to
10 the network by multiple people.
11 **Q. Isn't that a point of CX 19?**
12 A. Yes.
13 **Q. Mr. Wallace, have you ever traveled to**
14 **Washington, D.C. to meet with the FTC?**
15 A. Yes.
16 **Q. When did you do that?**
17 A. I would say it would have been -- it would have
18 been after the CID was issued, but I'm not sure of the
19 exact date.
20 **Q. Would it also have been after the list of**
21 **companies was provided pursuant to the CID?**
22 A. Yes. That was the purpose of the meeting, was
23 to clarify the -- how I put the data together, how it
24 would correspond with the list and the actual file.
25 JUDGE CHAPPELL: Is there any dispute as to this

1386

1 issue? If not, may he place the witness?
2 MS. VANDRUFF: I'm sorry, Your Honor. I don't
3 understand the question.
4 JUDGE CHAPPELL: Is there a dispute as to when
5 he came to visit with the FTC?
6 MS. VANDRUFF: I don't believe there's another
7 witness who has testified about when he came to meet
8 with the FTC, so I actually -- I don't --
9 JUDGE CHAPPELL: All right.
10 BY MR. SHERMAN:
11 **Q. You testified that the purpose of the meeting**
12 **was to discuss the information provided pursuant to the**
13 **CID; is that correct?**
14 A. Yes.
15 **Q. And do you recall who was at the meeting?**
16 A. There were multiple people. I mean, I don't --
17 I don't remember specific -- I do remember Alain was
18 there.
19 **Q. Alain who?**
20 A. Alain Sheer.
21 **Q. How long did the meeting last?**
22 A. Gosh, it's been so long ago. A couple of hours
23 maybe.
24 **Q. And was there any discussion of particular**
25 **companies that appeared on the list? And -- and don't**

1387

1 **name them if there was.**
2 A. Well, all of them would have been discussed. I
3 mean, it was something where you could look at the list
4 and then say okay, this is a file that corresponds with
5 this entry.
6 **Q. Was LabMD specifically discussed?**
7 A. Was LabMD on the list?
8 **Q. Were they specifically discussed that day, if**
9 **you remember, at the meeting with the FTC?**
10 A. I don't remember.
11 **Q. How did you get to D.C.?**
12 A. There was a previous commitment that we just
13 worked in an afternoon meeting. There was I believe
14 four of us that came from Tiversa.
15 **Q. Who traveled to D.C. from Tiversa?**
16 A. Bob Boback was driving. I was in the car,
17 Anju Chopra and Keith Tagliaferri.
18 **Q. Following the meeting, did the people from**
19 **Tiversa have discussions about the meeting?**
20 A. Yeah. I mean, we -- Bob spoke to me about next
21 steps on the way home.
22 **Q. And what were the next steps?**
23 MS. VANDRUFF: Object to the extent that it's
24 being offered for the truth of the matter asserted.
25 MR. SHERMAN: It's background as to what the

1388

1 next steps were, Your Honor. It's not based on the
2 truth of what --
3 JUDGE CHAPPELL: Not for the truth?
4 MR. SHERMAN: It's not for the truth.
5 JUDGE CHAPPELL: Overruled.
6 MR. SHERMAN: He said what the next steps were,
7 and I want to know what was discussed.
8 MS. VANDRUFF: Your Honor, I'm sorry. Just to
9 be clear, the testimony is permitted but not admitted
10 for its truth; is that correct?
11 JUDGE CHAPPELL: He said it's not for the truth.
12 Therefore, by definition, it is not hearsay.
13 MS. VANDRUFF: Thank you, Your Honor.
14 BY MR. SHERMAN:
15 **Q. You said there were next steps discussed.**
16 **What were the next steps discussed?**
17 A. Bob had indicated to me that the files needed to
18 have spread on them, you know, basically look for them
19 and see if they are available at other IP addresses, and
20 if they're not, make them appear to have -- you know, be
21 at different IP addresses.
22 **Q. In taking the next steps following the meeting**
23 **with the FTC, did you search for the insurance aging**
24 **file associated with LabMD?**
25 A. I did not.

1441

1 **analyst at Tiversa, who actually found that file;**
2 **correct?**
3 A. Yes. I downloaded that file.
4 **Q. And at the time you found the file, you also**
5 **found other documents along with it.**
6 A. Yes. But I downloaded the file and the other
7 documents on a stand-alone machine. I did not use
8 Tiversa's system, so I didn't find it in the data store.
9 I found it live online.
10 **Q. But after you found it live online, you**
11 **actually inputted that information into the Tiversa**
12 **data store.**
13 A. Yes.
14 **Q. And just to make sure we're clear on exactly**
15 **what a data store is, Tiversa maintained a record of the**
16 **files that it actually found along with files that it**
17 **wanted to create the appearance that they were found in**
18 **other locations on the Internet.**
19 A. Right.
20 **Q. Now, with respect to the 1718 File, I believe**
21 **you indicated this morning that you found this file in**
22 **February of 2008. Correct?**
23 A. Yes. February 25.
24 **Q. And at the time you found that file, is there**
25 **any doubt in your mind that this file was found on a**

1442

1 **LabMD computer in Atlanta, Georgia?**
2 A. Yeah -- well, after I downloaded the file, I
3 immediately went and browsed the host because I wanted
4 to get any other piece of information that would be at
5 that IP address, because when you pull open a PDF and
6 it's packed full of, you know, 8,000 people's healthcare
7 information or however many that are in there, chances
8 are there's other information there that would be
9 valuable as well.
10 **Q. And after you found this file in February 2008,**
11 **did you tell Mr. Boback that you found this?**
12 A. Yes. Within just a few minutes of opening it,
13 he was standing over my shoulder looking at it.
14 **Q. And when you showed this file to Mr. Boback,**
15 **what did he do next? Did he do anything himself or did**
16 **he direct you to do anything?**
17 A. He was very excited and told me that he was
18 going to take the lead on it.
19 **Q. I'm sorry. He was going?**
20 A. He was going to take the lead on it. He was
21 going to make contact with LabMD.
22 **Q. And do you know if he actually contacted LabMD?**
23 A. I would imagine he probably did. I mean, I was
24 not in the room.
25 **Q. But do you know today whether he has contacted**

1443

1 **LabMD?**
2 A. I would say yes.
3 **Q. Have you heard conversations in the Tiversa**
4 **offices about contacts that Mr. Boback made with LabMD?**
5 A. Yes.
6 **Q. Did LabMD ever hire Tiversa to do anything for**
7 **them?**
8 A. No.
9 **Q. So they did not accept Boback's proposal to**
10 **remediate their problem.**
11 A. No.
12 **Q. Was LabMD ever told by Tiversa where their file**
13 **had been found on the peer-to-peer networks?**
14 A. I believe that the initial contact, there was no
15 identifying information as far as the location on it. I
16 think it was the usual sales pitch where, if you pay us,
17 we can go look, but we don't know right now.
18 And then I think that there was a subsequent
19 e-mail that went out. After things went cold, Bob
20 reached back out to LabMD that, hey, your files --
21 either your files are being searched for or it is being,
22 you know -- it's spread all over the peer-to-peer space
23 and you need to remediate it.
24 **Q. But that wasn't true, was it?**
25 A. No.

1444

1 **Q. In fact, the file was never -- never spread**
2 **anywhere on the Internet.**
3 A. No. No. The originating source in Atlanta is
4 the only source that it's ever been seen at.
5 **Q. Now, there was a lot of talk this morning about**
6 **IP addresses that you provided to Mr. Boback, and at**
7 **least four of them were found on a document that has**
8 **been discussed today as CX 19; correct?**
9 A. Yes.
10 **Q. Now, these were not the only IP addresses that**
11 **Tiversa used to make it appear that files spread to**
12 **other locations on the Internet.**
13 A. No.
14 **Q. Do you have any idea today of approximately how**
15 **many different IP addresses that may have been used by**
16 **Tiversa to make it appear as though files were spread on**
17 **the Internet?**
18 A. I would say approximately twenty.
19 **Q. Twenty?**
20 A. Twenty.
21 **Q. And were there certain IP addresses that you**
22 **seemed to use more frequently than others?**
23 A. Yes.
24 **Q. And why was that?**
25 A. Like we were talking about this morning, if you

Notice of Electronic Service

I hereby certify that on August 30, 2016, I filed an electronic copy of the foregoing RESPONDENT LabMD, INC.'S APPLICATION FOR STAY OF FINAL ORDER PENDING REVIEW BY A UNITED STATES COURT OF APPEALS, with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on August 30, 2016, I served via E-Service an electronic copy of the foregoing RESPONDENT LabMD, INC.'S APPLICATION FOR STAY OF FINAL ORDER PENDING REVIEW BY A UNITED STATES COURT OF APPEALS, upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org

Respondent

Alain Sheer
attorney
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
General Attorney
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Attorney
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Attorney
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Alfred Lechner
President & CEO
Cause of Action Institute
jlechner@causeofaction.org
Respondent

Patrick Massari
Attorney