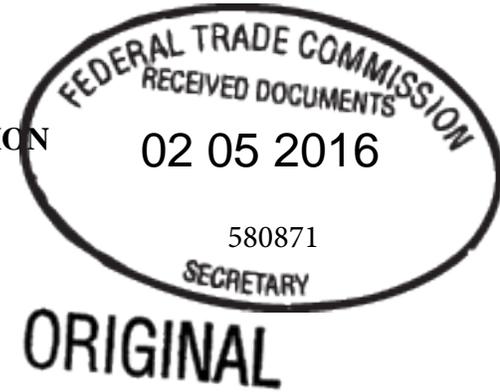


UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION



COMMISSIONERS: EDITH RAMIREZ, CHAIRWOMAN  
MAUREEN K. OHLHAUSEN  
TERRELL MCSWEENEY

\_\_\_\_\_)  
In the Matter of )  
)  
LabMD, Inc. )  
a corporation, )  
Respondent. )  
)  
\_\_\_\_\_)

**PUBLIC**

Docket No. 9357

**RESPONDENT LABMD, INC.'S CORRECTED<sup>1</sup> ANSWERING BRIEF**

Alfred J. Lechner, Jr.  
Daniel Z. Epstein  
Patrick J. Massari  
Cause of Action Institute  
1919 Pennsylvania Avenue, NW  
Suite 650  
Washington, DC 20006

Dated: February 5, 2016

*Counsel for Respondent*

\_\_\_\_\_  
<sup>1</sup> Respondent's Corrected Answering Brief replaces the earlier version submitted through the FTC E-Filing System.

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	v
RECORD REFERENCES AND GLOSSARY .....	xiii
STATUTES.....	ix
REGULATIONS.....	ix
OTHER AUTHORITIES.....	ix
I. INTRODUCTION IN RESPONSE TO THE FTC OPENING BRIEF.....	1
A. The FTC Prosecution of LabMD .....	1
B. Summary of Complaint and Answer.....	5
C. Summary of facts .....	5
1. Summary of some findings of fact.....	5
(a) Dr. Hill .....	5
(b) Credibility findings.....	6
(i) Fact witnesses .....	6
(c) Weight given to expert witnesses .....	7
D. Evidence and Summary of Initial Decision .....	7
E. Summary of argument.....	7
F. Procedural history .....	10
G. Question presented.....	10
II. ARGUMENT .....	11
A. The Initial Decision Is Correct As A Matter Of Law .....	11
1. Chief ALJ Chappell’s Findings of Fact, determinations of witness credibility, and evidentiary rulings are entitled to deference by the Commission .....	11

(a)	Chief ALJ Chappell’s determinations of credibility should be accorded deference and should not be disturbed absent a clear abuse of discretion .....	11
2.	Section 45(n) of Title 15 U.S.C. is unconstitutionally void for vagueness and failed to provide due process and fair notice to LabMD of unlawful medical data security acts or practices in 2007-2008 .....	13
(a)	Section 45(n) Is Unconstitutionally Vague On Its Face .....	13
(b)	There were no Section 5(n) rules, regulations, or standards that were applicable to the LabMD medical data security practices from June 2007 to May 2008 .....	14
(c)	The plain reading of Section 5(n) demonstrates that it contains no standard regarding unfair or unreasonable acts or practices for medical data security.....	17
3.	The FTC allegations of “significant risk of concrete harm” do not satisfy the Complaint Counsel burden under Section 5(n) to prove by reliable, probative, and substantial preponderant evidence that the LabMD medical data security standards in 2007-2008 caused injury or are likely to cause substantial injury.....	18
(a)	An act or practice that raises a “significant risk of concrete harm” does not satisfy the Section 5(n) requirement that the LabMD medical data security in 2007-2008 caused injury or is likely to cause substantial injury .....	18
(b)	The FTC theory of liability <i>per se</i> and strict liability under Section 5(n) is erroneous as a matter of law .....	22
(i)	Liability <i>per se</i> and strict liability.....	22
(c)	The Complaint Counsel argument regarding “law of the case” fails.....	26
(i)	The “law of the case” doctrine: the FTC cannot rely on a pre-trial, non-merits decision of the Commission as controlling.....	29
4.	As a matter of law, CC failed to prove its theoretical case which was based on an <i>ad hoc</i> standard of unreasonableness .....	31
(a)	The FTC assertion that ‘unreasonableness’ <i>in vacuo</i> suffices to prove a Section 5(n) violation is erroneous as a matter of law .....	33

(b)	No basis in law exists for the FTC argument that “significant risk of concrete harm” is equivalent to likelihood of substantial injury under Section 5(n).....	34
5.	FTC theories of “exposure” and/or “disclosure” as proof that the LabMD medical data acts or practices in 2007-2008 caused injury or are likely to cause substantial injury pursuant to Section 5(n) are erroneous. ....	35
6.	The FTC arguments regarding the Section 5(n) standard of proof for likelihood of substantial injury fail as a matter of law.....	37
7.	The FTC failed to prove by preponderant evidence that the alleged LabMD medical data security acts or practices from June 2007 to May 2008 caused injury or are likely to cause substantial injury as a causative consequence of the Sacramento Incident.....	38
B.	The Initial Decision Is Correct Per the Evidence Presented At The Hearing.....	41
1.	Complaint Counsel failed to adduce qualified expert testimony as appropriate opinions necessary to prove that LabMD violated Section 5(n).....	41
(a)	Negligence standards as applied to Section 5(n) .....	41
(b)	FTC experts failed to offer reliable, probative, and substantial opinion evidence of actual harm or likelihood of substantial harm under Section 5(n).....	43
(i)	Expert testimony is required to prove unfairness under Section 5(n).....	43
(c)	FTC expert Raquel Hill failed to provide reliable, probative, and substantial opinion evidence of actual injury or likelihood of substantial injury under Section 5(n) .....	46
(i)	Dr. Hill failed to apply her opinion to the June 2007 to May 2008 time frame.....	46
(ii)	Dr. Hill’s Report and Testimony .....	48
(d)	The Kam expert opinion is not reliable, probative, or substantial and the ID correctly ruled the opinion should be accorded little or no weight .....	51
(i)	Rick Kam’s report and testimony .....	51

(e)	The Van Dyke expert opinion is not reliable, probative, or substantial and it was correctly ruled the opinion should be accorded little or no weight.....	54
(i)	The Van Dyke Report and Testimony .....	54
2.	The testimony of rebuttal expert Clay Shields does not cure the failure of Complaint Counsel to prove the LabMD medical data security practices, as alleged, caused injury or are likely to cause substantial injury .....	57
(a)	The Clay Shields rebuttal testimony failed to offer an opinion that the LabMD medical data security practices in 2007-2008 caused or are likely to cause substantial harm to consumers.....	59
3.	Citations to Georgia privacy law do not prove by reliable, probative, and substantial preponderant evidence that the LabMD medical data security practices as alleged in 2007-2008 caused or are likely to cause substantial injury to consumers.....	63
(a)	The FTC argument for Section 5(n) liability under theories of Georgia tort law fail .....	63
(i)	Unlawful conduct by Tiversa and FTC.....	64
(ii)	Georgia tort law and privacy.....	65
(b)	The FTC argument that a right to privacy in sensitive medical information satisfies Section 5(n)'s standards of proof by proxy is erroneous.....	65
	CONCLUSION.....	67
	CERTIFICATE OF SERVICE .....	1
	CERTIFICATE OF ELECTRONIC FILING.....	2

**TABLE OF AUTHORITIES**

**CASES**

*American Financial Services v. FTC*, 767 F.2d 957 (D.C. Cir. 1985) ..... 3

*Arista Records LLC v. Lime Group LLC*, 2011 U.S. Dist. LEXIS 47416  
(S.D.N.Y. Apr. 29, 2011).....54

*Arizona v. California*, 460 U.S. 605 (1983)..... 29

*Atlantic Richfield Co. v. FTC*, 546 F.2d 646 (5th Cir. 1977)..... 64

*Bennett v. Spear*, 520 U.S. 154 (1997) ..... 30

*Blakely v. Johnson*, 140 S.E.2d 857 (1965) ..... 43

*Blue Cross and Blue Shield of Ala. V. Weitz*, 913 F.2d 396 (11th Cir. 1990) ..... 18

*Brooks v. Outboard Marine Corp.*, 234 F.3d 89 (2nd Cir. 2000)..... 55

*Brown Shoe Co. v. United States*, 370 U.S. 294 (1962) ..... 44

*Caminetti v. United States*, 242 U.S. 470 (1917)..... 17

*Chapman v. P&G Distrib., LLC*, 766 F.3d 1296 (11th Cir. 2004) ..... 6

*City of Los Angeles v. Lyons*, 461 U.S. 95 (1983) ..... 25

*Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) ..... 26

*Connally v Gen. Constr. Co.*, 269 U.S. 385 (1926) ..... 14

*Consolidated Bank, N.A. v. United States Dep’t of the Treasury, Office of the Comptroller*,  
118 F.3d 1461 (11th Cir. 1997) ..... 17

*Consumer Prod. Safety Comm’n v. GTE Sylvania*, 447 U.S. 102 (1980)..... 17, 18

*Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993)..... 45

*Daubert v. Merrell Dow Pharms.*, 43 F.3d 1311 (9th Cir. 1995) ..... 46

*FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012)..... 14

*FDIC v. Meyer*, 510 U.S. 471 (1994) ..... 35

<i>Focus on the Family v. Pinellas Suncoast Transit Auth.</i> , 344 F.3d 1263 (11th Cir. 2003).....	25
<i>FTC v. Accusearch, Inc.</i> , 2007 U.S. Dist. LEXIS 74905 (D. Wyo. Sept. 28, 2007) .....	2, 28
<i>FTC v. Commerce Planet, Inc.</i> , 878 F. Supp. 2d 1048 (C.D. Cal. 2012) .....	3
<i>FTC v. Dinamica Financiera LLC</i> , 2010 U.S. Dist. LEXIS 88000 (C.D. Cal. Aug. 19, 2010).....	36
<i>FTC v. Direct Benefits Group, LLC</i> , 2013 U.S. Dist. LEXIS 100593 (M.D. Fla. July 18, 2013).....	2
<i>FTC v. Inc21.com Corp.</i> , 745 F. Supp. 2d 975 (N.D. Ca. 2010) .....	2
<i>FTC v. Neovi, Inc.</i> , 598 F. Supp. 2d 1104 (N.D. Ga. 1974) .....	2, 3, 64
<i>FTC v. Page</i> , 378 F. Supp. 1052 (S.D. Cal. 2008) .....	64
<i>FTC v. Windward Mktg., Ltd.</i> , 1997 U.S. Dist. LEXIS 17114 (N.D. Ga. Sept. 30, 1997).....	3
<i>FTC v. Wyndham Worldwide Corp.</i> , 799 F.3d 236 (3rd Cir. 2015) .....	3, 53
<i>Gen. Electric v. Joiner</i> , 522 U.S. 136 (1997) .....	45
<i>Gonzalez v. McNary</i> , 980 F.2d 1418 (11th Cir. 1993).....	17, 18
<i>Heater v. FTC</i> , 503 F.2d 321 (9th Cir. 1974) .....	24
<i>Hudgins v. City of Ashburn</i> , 890 F.2d 396 (11th Cir. 1989).....	18
<i>In re Chicago Bridge &amp; Iron Co.</i> , 138 F.T.C. 1024 (Jan. 6, 2005) .....	32
<i>In re Int’l Harvester Co.</i> , No. 9147, 1984 FTC LEXIS 2 (F.T.C. Dec. 21, 1984) .....	<i>passim</i>
<i>In re Horizon Corp.</i> , No. 9017, 97 F.T.C. 464 (F.T.C. May 15, 1981).....	10, 11
<i>In re McWane, Inc.</i> , 2013 FTC LEXIS 76 (May 8, 2013).....	21, 45, 56
<i>In re Orkin Exterminating Co.</i> , 108 F.T.C. 263 (Dec. 15, 1986).....	5
<i>In re POM Wonderful, LLC</i> , FTC No. 9344, 2013 FTC LEXIS 6 .....	21, 22
<i>In re S. States Distrib. Co.</i> , 83 F.T.C. 1126 (1973) .....	12
<i>In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.</i> , 45 F. Supp. 3d 14 (D.D.C. 2014) .....	26

<i>In re Terazosin Hydrochloride Antitrust Litig.</i> , 352 F. Supp. 2d 1279 (S.D. Fla. 2005).....	44
<i>In the Matter of Certified Bldg. Prods., Inc.</i> , 83 F.T.C. 1004 (1973).....	13
<i>In the Matter of Gemtronics Inc.</i> , FTC No. 9330, 2009 FTC LEXIS 196 (Sept. 26, 2009).....	11
<i>Inv. Co. Inst. v. Camp</i> , 401 U.S. 617 (1971).....	30
<i>Knoll Associates v. FTC</i> , 397 F.2d 530 (7th Cir. 1968).....	64
<i>LabMD, Inc. v. FTC</i> , 2014 U.S. Dist. LEXIS 65090 (N.D. Ga. May 12, 2014) .....	39, 42
<i>LabMD, Inc. v. FTC</i> , 776 F.3d 1275 (11th Cir. 2015).....	30
<i>Loggerhead Turtle v. City Council</i> , 148 F.3d 1231 (11th Cir. 1998) .....	25
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992) .....	25
<i>Mercantile Tex. Corp. v. Bd. of Governors of Fed. Reserve Sys.</i> , 638 F.2d 1255 (5th Cir. 1981).....	44
<i>Murphy v. Federal Deposit Ins. Corp.</i> , 208 F.3d 959 (11th Cir. 2000).....	29
<i>Nat'l Parks Conservation Ass'n v. Norton</i> , 504 U.S. 555 (1992).....	25
<i>NLRB v. Walton Mfg. Co.</i> , 369 U.S. 404 (1962) .....	12
<i>Oladeinde v. City of Birmingham</i> , 230 F.3d 1275 (11th Cir. 2000) .....	29
<i>Orkin Exterminating Co. v. FTC</i> , 849 F.2d 1354 (11th Cir. 1988) .....	2, 36
<i>Owens v. Wainwright</i> , 698 F.2d 1111 (11th Cir. 1983).....	12
<i>Perez-Ruiz v. Crespo-Guillen</i> , 25 F.3d 40 (1st Cir. 1994).....	29
<i>Pride v. BIC Corp.</i> , 218 F.3d 566 (6th Cir. 2000) .....	45
<i>Prieto v. Malgor</i> , 361 F.3d 1313 (11th Cir. 2004).....	6
<i>Reilly v. Ceridian Corp.</i> , 664 F.3d 38 (3rd Cir. 2011).....	26, 35
<i>Riley v. Camp</i> , 130 F.3d 958 (11th Cir. 2011).....	29
<i>Remijas v. Neiman Marcus Grp., LLC</i> , No. 14-3122, 2015 U.S. App. LEXIS 12487 (7th Cir. 2015).....	53

<i>Resnick v. Av-Med, Inc.</i> , 693 F.3d 1317 (11th Cir. 2012) .....	23, 24, 66
<i>Riordan v. SEC</i> , 627 F.3d 1230 (D.C. Cir. 2010).....	24, 25
<i>Romero v. Drummond Co.</i> , 552 F.3d 1303 (11th Cir. 2008) .....	6
<i>Russell-Newman Mnfg. Co. v. N.L.R.B.</i> , 407 F.2d 247, 249 (5th Cir. 1969) .....	12
<i>Schering-Plough Corp. v. FTC</i> , 402 F.3d 1056 (11th Cir. 2005).....	12
<i>Shatel Corp. v. Mao Ta Lumber &amp; Yacht Corp.</i> , 697 F.2d 1352 (11th Cir. 1983) .....	44
<i>Smith v. Triad of Alabama, LLC</i> , No. 1:14-cv-324-WKW-PWG, 2015 U.S. Dist. LEXIS 132514 (M.D. Ala. Sept. 2, 2015).....	26, 66
<i>Southwest Sunsites v. FTC</i> , 785 F.2d 1431 (9th Cir. 1985).....	35, 36
<i>Thiret v. FTC</i> , 512 F.2d 176 (10th Cir. 1975).....	13
<i>Thompson v. Nagle</i> , 118 F.3d 1442 (11th Cir. 1997) .....	12
<i>United States v. Bonds</i> , 12 F.3d 540 (6th Cir. 1993) .....	45, 47
<i>United States v. Lebowitz</i> , 676 F.3d 1000 (11th Cir. 2012).....	12
<i>United States v. Marine Bancorporation, Inc.</i> , 418 U.S. 602 (1974).....	44
<i>United States v. Robinson</i> , 690 F.2d 869 (11th Cir. 1982).....	29, 30, 31
<i>Universal Camera Corp. v. NLRB</i> , 340 U.S. 474 (1951) .....	12
<i>Venn v. St. Paul Fire &amp; Marine Ins. Co.</i> , 99 F.3d 1058 (11th Cir. 1996) .....	29
<i>Villeda Aldana v. Del Monte Fresh Produce N.A., Inc.</i> , 578 F.3d 1283 (11th Cir. 2009) .....	29
<i>Vintilla v. United States</i> , 931 F.2d 1444 (11th Cir. 1991) .....	29
<i>Ward v. NLRB</i> , 462 F.2d 8 (5th Cir. 1972).....	12
<i>William Bros. v. Pate</i> , 833 F.2d 261 (11th Cir. 1987) .....	30
<i>Wooden v. Bd. of Regents</i> , 247 F.3d 1262 (11th Cir. 2001) .....	25
<i>Zenith Elecs. Corp. v. WH-TV Broad. Corp.</i> , 395 F.3d 416 (7th Cir. 2005).....	45, 46

*Zwiren v. Thompson*, 578 S.E.2d 862 (Ga. 2003)..... 43

**STATUTES**

5 U.S.C. § 556(d) ..... 31  
15 U.S.C. § 18..... 44  
15 U.S.C. § 45(l)..... 25  
15 U.S.C. § 45(n) ..... 10  
42 U.S.C. § 1320d-6 ..... 37, 64

**REGULATIONS**

16 C.F.R. § 3.31A(c) ..... 6  
45 C.F.R. Parts 160..... 48  
45 C.F.R. Parts 162..... 48  
45 C.F.R. Parts 164..... 48  
68 Fed. Reg. 8334 .....48  
68 Fed. Reg. 8338-49..... 48  
68 Fed. Reg. 8351 ..... 48  
68 Fed. Reg. 8359-64..... 48  
68 Fed. Reg. 8367-69..... 48  
68 Fed. Reg. 8372-73..... 48

**OTHER AUTHORITIES**

Dissenting Statement of Commissioner, J. Thomas Rosch re FTC File No. 1023099  
(June 21, 2012).....9  
*In the Matter of ECM BioFilms, Inc., a corporation, also d/b/a Enviroplastics International*, FTC  
No. 9358, Partial Dissent of Comm’r Maureen K. Ohlhausen at 7 .....44  
Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, div. A, title  
XIII, div. B, title IV, Feb. 17, 2009, 123 Stat. 226, 467 (42 U.S.C. 300jj et seq.; 17901 et seq.)  
(Feb. 17, 2009).....47, 48

H.R. CONF. REP. 103-617.....	42
H.R. REP. NO. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983) .....	5
P130500, Federal Trade Commission Minute: Ratification of Appointment of Administrative Law Judge and Chief Administrative Law Judge (Sept. 11, 2015) .....	11
S. REP. 103-130 (1993).....	5, 42

## **RECORD REFERENCES AND GLOSSARY**

ALJ – Administrative Law Judge

Boback – Robert Boback, Chief Executive Officer of Tiversa Holding Corp. and Tiversa, Inc.

CA – Closing Argument (September 16, 2015)

CC – Complaint Counsel

CCCL – Complaint Counsel’s Conclusions of Law

CCFF – Complaint Counsel’s Findings of Fact

CCB – Complaint Counsel’s Corrected Post-Trial Brief

CCOB – Complaint Counsel’s Opening Brief

CRRCL – Complaint Counsel’s Response to Respondent’s Conclusions of Law

CCRRFF – Complaint Counsel’s Response to Respondent’s Findings of Fact

CCRB – Complaint Counsel’s Post-Trial Reply Brief

CCX – Complaint Counsel’s Exhibit

CEO – Chief Executive Officer

Chief ALJ or Chief ALJ Chappell – FTC Chief Administrative Law Judge D. Michael Chappell

CLEAR – Consolidated Lead Evaluation and Reporting) is an investigative software database program, provided by Thompson Reuters Corporation that is used by investigators at the Federal Trade Commission to obtain information on individuals and corporations

CX – Complaint Counsel’s Exhibit

CX0000 (Witness, Dep.) at xx – Citations to deposition testimony

CX0000 (Witness, Exp. Rep.) at xx – Citations to expert reports

Dep. – Transcript of Deposition

F. – Findings of Fact contained in the Initial Decision

FJS – Final Joint Stipulations (JX001) (May 14, 2014)

FTC – Federal Trade Commission

GLBA – Gramm-Leach-Bliley Act

ID or Initial Decision – Initial Decision of Chief Administrative Law Judge D. Michael Chappell dated November 13, 2015

IDFF – Initial Decision Findings of Fact

IPC – Initial Pretrial Conference held September 25, 2013

JX – Joint Exhibit

LabMD – LabMD, Inc.

LabMD Dep. – Rule 3.33 deposition of Michael J. Daugherty in his capacity as President and Chief Executive Officer of LabMD, Inc. (March 4, 2014)

OS – Opening Statement (May 20, 2014)

PIH – Hearing on LabMD’s Motion for Preliminary Injunction (*LabMD, Inc. v. FTC*, Civil Action File No. 1:14-CV-810-WSD (U.S. Dist. Court for the N. Dist. of GA – Atlanta Div’n)) (May 9, 2014)

PNO – Proposed Notice Order

RB – Respondent’s Corrected Post-Trial Brief

RCL – Respondent’s Corrected Conclusions of Law

Respondent – LabMD, Inc.

RFF – Respondent’s Findings of Fact

RPTB – Respondent’s Post-Trial Brief

RRB – Respondent’s Post-Trial Reply Brief

RRCL – Respondent’s Reply to Complaint Counsel’s Conclusions of Law

RRCFF – Respondent’s Reply to Complaint Counsel’s Findings of Fact

RX – Respondent’s Exhibit

Section 45(n) – 15 U.S.C. § 45(n)

Section 5(n) – 15 U.S.C. § 45(n)

Tiversa – Tiversa Holding Corp. or Tiversa, Inc.

Tr. – Transcript of testimony before the Administrative Law Judge

Witness, Dep. 0000 – Citations to deposition testimony

Witness, Rep. 0000 – Expert report of witness

Witness, Rebuttal Rep. 0000 – Expert rebuttal report of witness

Witness, Tr. 0000 – Citations to trial testimony

I. INTRODUCTION IN RESPONSE TO THE FTC OPENING BRIEF

A. The FTC Prosecution of LabMD

The FTC case against LabMD under Section 5(n) of the Federal Trade Commission Act is based upon abstractions, possibilities, and speculation. At the commencement of trial, LabMD, in its opening statement, pointed out the inability of CC to prove its case under the statute:

MR. SHERMAN: [I]t appears that this case is more about what could have happened, it's more about what might happen, what might have happened, but it's certainly not about what happened. And the evidence will show that the government is unable to establish the link between what they allege are LabMD's data security practices and any harm to any consumer.

JUDGE CHAPPELL: What about the likelihood of harm?

MR. SHERMAN: I submit to the court that the evidence will be deficient in connecting LabMD's alleged data security practices and the likelihood of harm. And I submit to the court that that is precisely what they will be unable to prove.

OS at 51.

Chief Administrative Law Judge D. Michael Chappell ruled on November 13, 2015 in his Initial Decision that CC 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 [CC] has failed to prove the first prong of the three-part test [under Section 5(n)] – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers." ID at 13. The Chief ALJ commented that this case is merely "theory" because FTC never set forth medical data security standards regarding unfair acts or practices applicable to LabMD from June 2007 to May 2008 under Section 5(n).

No standard existed in 2007-2008 under Section 5(n) regarding what constituted unfair medical data security practices for small businesses like LabMD. Moreover, CC conceded that no actual harm exists in this case. *See* CA at 11-13 (JUDGE CHAPPELL: “And how many have – how many came forward? How many have you identified that said they were harmed?” MS. VANDRUFF: “Your Honor, if your question is how many consumers have identified that they were harmed as a proximate cause of LabMD’s actions, conduct –” JUDGE CHAPPELL: “I’m asking you as the person who prosecuted the case.” MS. VANDRUFF: “Yes, Your Honor.” JUDGE CHAPPELL: “How many did you bring forward?” MS. VANDRUFF: We did not present a consumer witness in this case, Your Honor.”).

As the Chief ALJ recognized: “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.” *See* ID at 53 (citing *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (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), *cert. denied*, 488 U.S. 1041 (1989); *FTC v. Direct Benefits Group, LLC*, 2013 U.S. Dist. LEXIS 100593, at \*39-40 (M.D. Fla. July 18, 2013) (payments to Defendants of more than \$9.5 million after accounting for returns, refunds, and chargebacks); *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975, 1003-1004 (N.D. Ca. 2010) (\$37 million in largely unauthorized charges flowed directly to defendants); *FTC v. Accusearch, Inc.*, 2007 U.S. Dist. LEXIS 74905, at \*23-24 (Sept. 28, 2007) (“documented economic harm” in the form of “actual costs associated with changing telephone carriers and addressing necessary upgrades to the security of the accounts”), *aff’d*, 570 F.3d 1187 (10th Cir. 2009); *FTC v. Neovi*,

*Inc.*, 604 F.3d 1150, 1154 (9th Cir. 2010) (defendant operated a website through which various con artists and fraudsters drew over 150,000 bad checks totaling over \$400 million, caused by the defendant's faulty "Qchex" system); *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (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); *FTC v. Windward Mktg., Ltd.*, 1997 U.S. Dist. LEXIS 17114, at \*1-22, \*31-32 (N.D. Ga. Sept. 30, 1997) (unauthorized demand drafts paid against consumers' bank accounts as a result of fraudulent telemarketing scheme); *In re Int'l Harvester Co., a corporation*, 1984 FTC LEXIS 2, at \*255 (FTC No. 9147) (Dec. 21, 1984) (death and serious injury resulting from failure to disclose known defects in respondent's tractors); *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3rd Cir. 2015) ("On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over \$10.6 million dollars in fraudulent charges.").

There is no decision or binding precedent where a respondent was found to have violated Section 5(n) based only on allegations regarding possible risk of likely substantial harm. The cases cited by CC in support of its argument, including *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104 (S.D. Cal. 2008), all involve actual harm to consumers. *American Financial Services*, 767 F.2d 957 (D.C. Cir. 1985), is irrelevant because (1) it was decided in 1985, before the August 26, 1994 amendments creating Section 5(n); (2) the case involved rulemaking, not formal adjudication of unfair practices; and, (3) financial and other actual harm to consumers occurred. *See* ID at 55 n.26.

If Congress intended “significant risk of concrete harm” to be a basis to find actual injury or likely substantial injury, it would have included that language in the statute. Congress did not do so. A plain reading of Section 5(n) supports LabMD’s position in on this issue.

At a May 2014 preliminary injunction hearing in the Northern District of Georgia, Judge William S. Duffey, Jr. stated the following regarding the FTC interpretation of Section 5(n) (FTC official Robert Schoshinski, Assistant Director in the Division of Privacy and Identity, was present):

[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 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 they – after-hand.

PIH Tr. at 94-95.

“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.” ID at

14.

“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.’” Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (Mar. 5, 1982), reprinted in H.R. REP. NO. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983). Furthermore, “[i]n adopting Section 5(n), Congress noted: ‘In most cases, substantial injury would involve monetary or economic harm or unwarranted health and safety risks.’” See S. REP. 103-130, 1993 WL 322671, at \*13. “[A]lthough a finding of unfair conduct can be based on ‘likely’ future harm, ‘[u]nfairness cases usually involve actual and completed harms.’” ID at 48 (citing *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)).

B. Summary of Complaint and Answer

LabMD adopts the Summary of Complaint and Answer set forth in the ID. See ID at 1-5.

C. Summary of facts<sup>2</sup>

LabMD adopts the Findings of Fact set forth in the ID. See ID at 15-44 ¶¶ 1-258.

1. Summary of some findings of fact

(a) Dr. Hill

- At trial, Chief ALJ Chappell excluded from evidentiary consideration the Hill testimony regarding increased risk of data exposure as a result of the LabMD data security practices. She was barred from opining on whether LabMD’s data security practices caused risk of harm because such an opinion from Dr. Hill was outside of the scope of

---

<sup>2</sup> To the extent the CC Statement of Facts conflicts with either the IDFF, and/or RFF or RCFF, Respondent adopts the IDFF.

her expert report, which only assessed whether LabMD’s data-security was “reasonable.”<sup>3</sup> Tr. at 319-22; *accord* Rule 3.31A(c), 16 C.F.R. § 3.31A(c), states: “Each report shall be signed by the expert and contain a complete statement of all opinions to be expressed and the basis and reasons therefor . . .”); Additional Provision of Scheduling Order 19(d).

(b) Credibility findings

(i) Fact witnesses

- On eight occasions in the Initial Decision, Chief ALJ Chappell made specific credibility or demeanor determinations regarding two key witnesses: Robert Boback and Richard Wallace. ID at 8 n.7; 33-34 ¶¶ 155, 160, 167-68; 60-61; 91 ¶ 26.
  - The Chief ALJ found Boback to be “unreliable, not credible, and outweighed by credible contrary testimony from Mr. Wallace; due to Boback’s “biased motive, [he] is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of Respondent.” *Id.* at 33 ¶¶ 156-159.
  - “Based on Mr. Wallace’s forthrightness in response to questioning, and his overall demeanor observed during his questioning, Mr. Wallace is a credible witness.” *Id.* at ¶ 155.
- The Chief ALJ found that evidence and testimony provided by Tiversa was entitled to no weight. ID at 60.

---

<sup>3</sup> Moreover, Dr. Hill was never asked to opine within a reasonable degree of probability/likelihood whether LabMD medical data security during the relevant time period proximately caused injury or was likely to cause substantial injury. The FTC’s argument is also wrong as a matter of law. *See Romero v. Drummond Co.*, 552 F.3d 1303, 1323-24 (11th Cir. 2008); *Chapman v. P&G Distrib., LLC*, 766 F.3d 1296, 1312-16 (11th Cir. 2014). *See generally Prieto v. Malgor*, 361 F.3d 1313, 1317-18 (11th Cir. 2004) (describing general requirements for Rule 26 expert reports).

- On five occasions in the Initial Decision, Chief ALJ Chappell made credibility findings regarding FTC key evidence, CX 19 (false evidence of “spread”), and Tiversa’s “data store.” ID at 29 ¶ 120; 33 ¶ 159; 60-61; 91 ¶ 26.
  - The Chief ALJ found that CX0019 was “not credible or reliable evidence to show that the 1718 File spread on any peer-to-peer network.” *Id.* at 33 ¶ 159.
  - Chief ALJ Chappell found that “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.” *Id.* at 29 ¶120.

(c) Weight given to expert witnesses

- On four occasions, the Chief ALJ expressly found that Kam’s conclusions are entitled to little or no weight. ID at 61, 68, 76, 79.
- On at least two occasions, the Chief ALJ describes Van Dyke’s testimony as “speculation.” ID at 64, 66.
- On at least three occasions, the Chief ALJ describes Van Dyke’s testimony as “unpersuasive.” ID at 64, 80.
- Mr. Van Dyke did not conduct a survey of the consumers listed on the 1718 File. ID at 64 (citing F. 255).

D. Evidence and Summary of Initial Decision

LabMD adopts the statements regarding Evidence, and Summary of Initial Decision set forth in the ID. *See* ID at 11-14.

The Initial Decision is correct as a matter of fact and as a matter of law.

E. Summary of argument

The Conclusion of Chief Judge Chappell in the Initial Decision succinctly stated:

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.

ID at 87.

The FTC case against LabMD was based on two “security incidents” that were never properly investigated by the FTC. The FTC prosecution of LabMD was based upon the theft of the 1718 File by Tiversa from a LabMD workstation in Atlanta, Georgia in February 2008. Wallace Tr. at 1337-1355; 1358-1396; 1398-1458. The information and testimony from Boback and Tiversa that the CC proffered as evidence of likely substantial harm was based on deceit and fraud. The crime (the theft of the 1718 File from LabMD by Tiversa), and the lie (that the 1718 File had “spread” to four or more IP addresses) undercut the FTC case.

Additionally, CC “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, [CC] 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.” ID at 72.

The LabMD filings directed CC and FTC to then-Commissioner J. Thomas Rosch's Dissent from Commissioner Brill's April 20, 2012 decision denying Respondent's Motion to Quash or Limit Civil Investigative Demand. *See* 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>. The LabMD Motion To Disqualify Commissioner Edith Ramirez cited Commissioner Rosch's warning:

On June 21, 2012, Commissioner J. Thomas Rosch prophetically warned FTC about Tiversa, stating "I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File." He went on to note FTC's obvious conflict of interest in blindly relying upon "a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks."

FTC should have listened.

LabMD's Motion To Disqualify Commissioner Edith Ramirez (Apr. 27, 2014) (PUBLIC) at 1-2.

In the Procedural Summary subsection in the Initial Decision, Chief ALJ Chappell stated that CC and other 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." ID at 7. CC ignored due diligence and reasonable caution in favor of a blind pursuit of LabMD based on evidence CC knew, or should have known, was tainted and unreliable.

Years have passed since the alleged "security incidents" involving the 1718 File and the Sacramento "Day Sheets." FTC did not receive one complaint about LabMD data security practices in 2007-2008. No victim has come forward with a complaint attributable to LabMD,

the 1718 File, or the Day Sheets. Moreover, there is no evidence that likely substantial harm will occur based on the allegations in the Complaint.

The Initial Decision is correct as a matter of fact and as a matter of law; it should be affirmed.

F. Procedural history

LabMD adopts the Summary of Complaint and Answer set forth in the ID. *See* ID at 5-11. LabMD also adopts all of its post-trial briefings in this case: RFF; RCL; RB; RCFF; RRCL; and, RRB. LabMD further adopts its briefing and reply in opposition to the Proposed Notice Order.

G. Question presented

Based on a consideration of the entire Record relevant to the issues, whether the FTC proved under 15 U.S.C. § 45(n) (“5(n)”) of the Federal Trade Commission Act by reliable, probative, and substantial preponderant evidence that LabMD medical data security acts or practices from June 2007 to May 2008 caused or are likely to cause substantial injury to consumers.

## II. ARGUMENT

### A. The Initial Decision Is Correct As A Matter Of Law

1. Chief ALJ Chappell's Findings of Fact, determinations of witness credibility, and evidentiary rulings are entitled to deference by the Commission
  - (a) Chief ALJ<sup>4</sup> Chappell's determinations of credibility should be accorded deference and should not be disturbed absent a clear abuse of discretion

The Commission should not disturb the ALJ rulings as to credibility, weight, reliability, and disputed facts. Because the Chief ALJ observed witness testimony in person, his determinations of credibility should be accorded deference. *See In re Horizon Corp.*, No. 9017, 97 F.T.C. 464, 857 n.77 (F.T.C. May 15, 1981).

“[I]t is the [Chief ALJ], as trier of the facts, who has lived with the case, and who has had the opportunity to closely scrutinize witnesses' overall demeanor and to judge their credibility. Accordingly, absent a clear abuse of discretion, the Commission will not disturb on appeal the [Chief] ALJ's conclusions as to credibility.” *In the Matter of Gemtronics, Inc., a corporation*, FTC No. 9330, 2009 FTC LEXIS 196, at \*88 (Sept. 26, 2009), *aff'd*, 151 FTC 132, 2011 FTC LEXIS 68 (Feb. 11, 2011) (quoting *In re Horizon Corp.*, No. 9017, 97 F.T.C. 464, 856 n.77 (F.T.C. May 15, 1981), (FTC did not appeal Chief ALJ Chappell's ruling regarding deference to the ALJ's conclusions as to credibility absent a clear abuse of discretion); *accord In re Trans Union Corp.*, No. 9255, 2000 FTC LEXIS 23, at \*9 (Feb. 10, 2003). “The Supreme Court has

---

<sup>4</sup> On September 11, 2015, on Motion by Chairwoman Ramirez, the Commission ratified the appointment of D. Michael Chappell as a Federal Trade Commission Administrative Law Judge and as the Commission's Chief Administrative Law Judge. *See* P130500, Federal Trade Commission Minute: Ratification of Appointment of Administrative Law Judge and Chief Administrative Law Judge (Sept. 11, 2015) (Chairwoman Ramirez, Commissioner Ohlhausen, and Commissioner McSweeney voted in the affirmative, and Commissioner Brill did not participate).

recognized the importance of an [ALJ's] determination of credibility, and explained that evidence which supports an administrative agency's fact-finding 'may be less substantial when an impartial, experienced examiner<sup>[1]</sup> who has observed the witnesses and lived with the case has drawn conclusions different from the agency's . . . .'" *Id.* (quoting *Schering-Plough Corp. v. FTC*, 402 F.3d 1056, 1070-71 (11th Cir. 2005) (quoting *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 487-88, 496 (1951))).

"Evaluation of witness credibility . . . is a matter for which the administrative law judge is best situated, and absent good cause to challenge that evaluation, we will not disturb it." *In re S. States Distrib. Co.*, 83 F.T.C. 1126, 1973 FTC LEXIS 253, at \*106-07 (1973); accord *NLRB v. Walton Mfg. Co.*, 369 U.S. 404, 408 (1962). In *Universal Camera*, the Court found that because of the hearing examiner's "opportunity to observe the witnesses," his decision "intrinsically commands" considerable "probative force." *Id.*<sup>5</sup>

"[W]hen the ultimate determination of motive or purpose hinges entirely upon the degree of credibility to be accorded the testimony of interested witnesses, 'the credibility findings of the Trial Examiner are entitled to special weight and are not to be easily ignored.'" *Ward v. NLRB*, 462 F.2d 8, 12 (5th Cir. 1972) (citing *Russell-Newman Mnfg. Co. v. N.L.R.B.*, 407 F.2d 247, 249 (5th Cir. 1969)). "The preeminence of [Chief ALJ Chappell's] conclusions regarding testimonial probity does not amount to an inflexible rule that either the [Commission] or a reviewing court

---

<sup>[1]</sup> "At the time of the opinion in *Universal Camera*, an 'examiner' performed the same functions as an ALJ." *Schering-Plough v. FTC*, 402 F.3d 1056, 1071 n.24 (11th Cir. 2005).

<sup>5</sup> Findings of fact in Article III trial courts are reviewed for clear error "even when the district court's findings are drawn solely from documents, records, or inferences from other facts." *Thompson v. Nagle*, 118 F.3d 1442, 1447 (11th Cir. 1997) (citations omitted); see also Fed. R. Civ. P. 52(a)(6); *United States v. Lebowitz*, 676 F.3d 1000, 1009 (11th Cir. 2012) (per curiam) ("Appellate courts reviewing a cold record give particular deference to credibility determinations of a fact-finder who had the opportunity to see live testimony." (quoting *Owens v. Wainwright*, 698 F.2d 1111, 1113 (11th Cir. 1983))).

must invariably defer to his decision, thereby effectively nullifying either administrative or judicial review. But when the [Commission] second-guesses the Examiner and gives credence to testimony which he has found – either expressly or by implication – to be inherently untrustworthy, the substantiality of that evidence is tenuous at best.” *Id.* (note omitted). The Chief ALJ “sees the witnesses and hears them testify, while the [Commission] and the reviewing court look only at cold records.” *Id.* at 12 n.6.

The Commission ordinarily “leave[s] undisturbed those findings of an ALJ derived from his observations of the demeanor of witnesses and the bearing this has on his evaluation of the character and quality of the testimony received at trial.” *In the Matter of Certified Bldg. Prods., Inc.*, 83 F.T.C. 1004, 1973 FTC LEXIS 250, at \*43 (1973), *aff’d sub nom.; Thiret v. FTC*, 512 F.2d 176, 179 (10th Cir. 1975).

2. Section 45(n) of Title 15 U.S.C. is unconstitutionally void for vagueness and failed to provide due process and fair notice to LabMD of unlawful medical data security acts or practices in 2007-2008

- (a) Section 45(n) Is Unconstitutionally Vague On Its Face

Section 5(n) is unconstitutionally vague on its face because the standard of care regarding “unfair” or “unreasonable” medical data security in 2007-2008 is undefined. It did not provide fair notice regarding what acts or practices would violate the statute.

This enforcement action violates due process because LabMD never received adequate notice of what PHI data-security practices it was required to, or prohibited from, implementing that are different from and in addition to those required by HIPAA, HITECH, and HHS regulations implementing those statutes. “[T]he void for vagueness doctrine addresses at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so

that those enforcing the law do not act in an arbitrary or discriminatory way.” *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (citation omitted).

Section 5(n) contains no standard of care regarding medical data security practices in 2007-2008. The statute’s general prohibition of “unfair” acts or practices is constitutionally vague; it does not provide adequate notice of the medical data security practices that it seeks to forbid or require. *See Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926).

- (b) There were no Section 5(n) rules, regulations, or standards that were applicable to the LabMD medical data security practices from June 2007 to May 2008<sup>6</sup>

FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing medical data security standards that have the force of law. *See IPC at 9-10, 21-22* (Sept. 25, 2013).

JUDGE CHAPPELL: [H]as the Commission issued guidelines for companies to utilize to protect this information or is there something out there for 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 . . .

JUDGE CHAPPELL: I’m not sure you answered my question, Counselor. 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?

---

<sup>6</sup> CC concedes that the ID is correct in finding the relevant time period in this case to be June 2007 to May 2008. *See ID at 60, 65* (“ . . . [T]he 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.”); CCOB at 4 (“The 1718 File was available on the P2P network for at least eleven months.”) (citations omitted), 8 (“eleven month period” for searches to be done on Limewire to locate the 1718 File).

MR. SHEER: [] No.

CC Alain Sheer admitted in his opening statement that the FTC case was based on a HIPAA statutory standard which was applicable to the LabMD medical data security practices and with which LabMD complied with during all relevant times.

JUDGE CHAPPELL: This defense in depth you're talking about, is this a law, regulation or guideline that's out there for everybody to see? . . . I'm talking about government only. My question goes to the government only.

MR. SHEER: Yes.

JUDGE CHAPPELL: Law, regulation or guideline published by the government.

MR. SHEER: There are guidelines that have been published, for example, having to do with the security of health information that have these same basic concepts built into them. They're not always called defense in depth, but there are a series of standard steps, which we're going to talk about, that will illustrate what "defense in depth" means.

JUDGE CHAPPELL: These guidelines have been published. Can you cite me to them right now?

MR. SHEER: I can point you to the – I can point you to pieces of it right now. I can point you to the HIPAA security rule which has – which lays out in some detail what defense in depth requires.

JUDGE CHAPPELL: Did you say HIPAA?

MR. SHEER: I did.

JUDGE CHAPPELL: Okay.

FTC OS at 18-19.

There are several problems with the CC statements here regarding HIPAA.

First, FTC stipulated it was not enforcing HIPAA in this case, during 2007-2008 or at any other relevant time. *See* FJS at 3 ¶ 7 (JX0001 – May 14, 2014) (“[CC] does not seek to enforce HIPAA in this case.”).

Second, the “defense-in-depth” standard articulated by the FTC and its expert Raquel Hill, which relies in part on HIPAA, was not applicable to medical data security from June 2007 to May 2008, and therefore is irrelevant to this case. *See* Hill, Tr. at 305-10. Dr. Hill was unaware of any document that cites all of her “seven principles for a comprehensive information security program.” RFF at 86 ¶ 362 (citing Hill, at Tr. 242-43). Most importantly, LabMD cannot be held to this “standard” because it was not established that such standard existed and was applicable to LabMD for the relevant time period. Moreover, Dr. Hill only became aware of the so-called defense-in-depth strategy circa mid-2009. *Id.* at ¶ 365 (citing Hill, Tr. 306).

Third, to the extent the FTC or its expert Raquel Hill relied on the Security Rule or other part of HIPAA to prove their case, they fail: LabMD was HIPAA-complaint at all relevant times, *see* LabMD Dep. at 119, and FTC stipulated it was not enforcing HIPAA. *See* FJS at 3 ¶ 7. CC also argues in its brief that LabMD somehow violated HIPAA or another statute because “LabMD did not notify the consumers whose information was contained in the 1718 File, depriving them of the knowledge that their most sensitive information had been exposed and the opportunity to identify and remedy the effects of that exposure.” CCOB at 4 (citing CCFF ¶ 1411). This argument is erroneous as a matter of law because (1) HITECH, the statute which requires such notification, was not enacted until February 17, 2009, after the theft of the 1718 File by Tiversa in the 2007-2008 time frame. *See* Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, div. A, title XIII, div. B, title IV, Feb. 17, 2009, 123 Stat. 226, 467 (42 U.S.C. 300jj et seq.; 17901 et seq.) (Feb. 17, 2009); and, (2) HHS intentionally

chose not to join the FTC prosecution of LabMD because LabMD did not violate HIPAA or HITECH: “An HHS spokesperson responded to [the] 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 no obligation on LabMD with respect to our breach notification requirements – whether any exist under state law would be for the state to determine.

RX0649 at 2-3 (PHIprivacy.net) (Sept. 9, 2013).

Finally, Dr. Hill was not offered as an expert on HIPAA; in fact, she admitted that she knows very little about the statute. *See Hill Tr.* at 231 (Q. “And would you agree that HIPAA is a regulation that governs the – in part, governs the storage and transfer of health-related information by medical care providers?” [Dr. Hill:] “I can’t make a statement or – about the legal aspects of HIPAA and what it governs. I don’t understand the legal aspects of what it governs.” Q. “So you’re not intimately familiar with HIPAA then.” [Dr. Hill:] “No, sir.”).

- c. The plain reading of Section 5(n) demonstrates that it contains no standard regarding unfair or unreasonable acts or practices for medical data security

“The starting point for interpreting a statute is the language of the statute itself.” *Consumer Prod. Safety Comm’n v. GTE Sylvania*, 447 U.S. 102, 108 (1980). As a basic rule of statutory interpretation, the statute is read “using the normal meanings of its words.” *Consolidated Bank, N.A. v. United States Dep’t of the Treasury, Office of the Comptroller*, 118 F.3d 1461, 1463 (11th Cir. 1997).

”The meaning of the statute must, in the first instance, be sought in the language in which the act is framed, and if that is plain . . . the sole function of the courts is to enforce it according to its terms.” *Gonzalez v. McNary*, 980 F.2d 1418, 1420 (11th Cir. 1993) (quoting *Caminetti v. United States*, 242 U.S. 470, 485 (1917)).

The FTC contends Congress codified part of a footnote from the 1980 Unfairness Standard when it enacted Section 5(n). *See* CCOB at 6, 13. However, if Congress intended “significant risk of concrete harm” to be the standard of proof for Section 5(n) unfairness violations, it would have included such language in the statute. *See* Section 5(n); *Hudgins v. City of Ashburn*, 890 F.2d 396, 405 (11th Cir. 1989); *see also Blue Cross and Blue Shield of Ala. v. Weitz*, 913 F.2d 1544, 1548 (11th Cir. 1990). It did not. A reference to legislative history or to what Congress might have meant or what IT could have meant is inappropriate. Section 5(n) does not contain the language the FTC urges upon the Commission. *See* CCOB at 7, 13-15, 16 n.5. “Alternative explanations” are not necessary when the language of Section 5(n) is clear. *See GTE Sylvania*, 447 U.S. at 108; *Gonzalez v. McNary*, 980 F.2d 1418, 1420 (11th Cir. 1993).

For this reason alone, the Commission should affirm the Initial Decision as a matter of law.

3. The FTC allegations of “significant risk of concrete harm” do not satisfy the Complaint Counsel burden under Section 5(n) to prove by reliable, probative, and substantial preponderant evidence that the LabMD medical data security standards in 2007-2008 caused injury or are likely to cause substantial injury
  - (a) An act or practice that raises a “significant risk of concrete harm” does not satisfy the Section 5(n) requirement that the LabMD medical data security in 2007-2008 caused injury or is likely to cause substantial injury

The FTC argument that an act or practice that raises a “significant risk of concrete harm” equates to a likelihood of substantial injury fails for several reasons.

First, a plain reading of Section 5(n) reveals that a “significant risk of concrete harm” is not part of the statute. Accordingly, the CC attempt to read that language/standard into Section 5(n) is erroneous as a matter of law.<sup>7</sup>

Second, “significant risk of concrete harm” appears as Footnote Twelve in the FTC 1980 Unfairness Statement. *See* Unfairness Statement, *reprinted in In re Int’l Harvester Co.*, 1984 LEXIS 2, at \*307 n.12 (F.T.C. Oct. 10, 1984). In amending the FTC Act in 1994 to include Section 5(n), Congress did not codify “significant risk of concrete harm” in any manner. Instead, the Section 5(n) proof requirements regarding injury are a “statutory limitation” on unfair acts or practices. *See* ID at 47-48 (citations omitted). The FTC argument is wrong because it attempts to broaden the language of the Section 5(n) definition of unfairness; it does not require proof by a preponderance of the evidence that the act or practice caused injury or is likely to cause injury.

Third, assuming *arguendo* that “significant risk of concrete harm” is a putative limitation pursuant to Section 5(n), the FTC failed to prove that the LabMD medical data security in 2007-2008 created such risk. *See* ID at 55 (“[E]ven 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.”). The FTC relies in part upon Mr. Kam’s opinion for support of the argument that “exposure of the 1718 File poses a significant risk of identity theft harm.” *Id.* at 61 (citing CX0742 (Kam Expert Report at 18-19)). However, Mr. Kam did not opine with a reasonable degree of likelihood/probability. Moreover, the Kam opinion is based upon the discredited testimony of Boback, which in turn renders the opinion unreliable, not credible, and not entitled to any weight. *Id.* But even so, “significant risk of concrete harm” is not the standard.

---

<sup>7</sup> *See supra* Section II.A.2.c.

The evidence shows that the 1718 File “was no longer available for sharing by LabMD as of May 2008, and the evidence fails to show that the 1718 File remained available on peer-to-peer networks after May 2008.” *Id.* at 62 (citations omitted). Under the Kam analysis, “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.” *Id.*

The testimony and opinions of both Mr. Kam and Mr. Van Dyke were based on the assumption that LabMD medical data security practices were inadequate and unreasonable. *See id.* at 43 ¶ 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, Exp. Rep. at 5); *id.* at 44 ¶ 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 Exp. Rep. at 2, 13); Van Dyke, Tr. 695-696).]” As a consequence, these opinions and testimony are unreliable and not probative.

The FTC also argues that based upon the testimony of Mr. Van Dyke, “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.” *See id.* at 63 (note omitted). The Van Dyke reliance upon the 2013 Javelin Survey and the 2014 Javelin Report is “not persuasive in proving that those consumers whose Personal Information was exposed in the 1718 File are likely to suffer identity theft harm.” *Id.* at 64. “[T]he 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 [Mr. Van Dyke's] expert opinion that such harm is, nonetheless, 'likely' to occur." *Id.* (citing *In re McWane, Inc.*, No. 9351, 2013 FTC LEXIS 76, at \*730-31 (F.T.C. May 8, 2013)).

The Van Dyke opinions on "significant risk" are unreliable, not probative, do not talk in terms of likelihood/probability, and are unpersuasive; as well they fail to make temporal and situational comparisons to the individuals in the 1718 File. "[T]he 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. The FTC 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." *Id.* at 65. Mr. Van Dyke's 2013 Javelin survey cannot be predictive of identity theft for the 1718 File population in May 2008.

Moreover, there is an absence of preponderant evidence 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." *Id.* The FTC acknowledged this problem in a recent case when it argued that "[t]he first step in evaluating a consumer survey is to consider whether it drew valid samples from an appropriate population." CC Appeal Brief at 13, *In re ECM BioFilms, Inc.*, (F.T.C. Oct. 19, 2015) (No. 9358) (citing *In re POM Wonderful, LLC*, No. 9344, 2013 FTC LEXIS 6, at \*49 (F.T.C. Jan. 10,

2013). Mr. Van Dyke violated the FTC rule of survey methodology, and his opinions were not, and should not, be given any weight for that reason alone.

The Kam reliance on the 2013 Ponemon Survey suffers from the same temporal and comparative defects as his reliance on the 2013 Javelin Survey and 2014 Javelin Report. Neither survey is probative evidence of the likelihood of substantial harm to the population of individuals within the 1718 File.

The FTC evidence fails to demonstrate that disclosure of the 1718 File to Tiversa has caused, or is likely to cause, identity theft harm, or that this disclosure raised a “significant risk of concrete harm.” Neither Chief ALJ Chappell nor the parties have cited 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.” ID at 55 (note omitted).

(b) The FTC theory of liability *per se* and strict liability under Section 5(n) is erroneous as a matter of law

(i) Liability *per se* and strict liability

Richard Wallace undercut the validity of the FTC case against LabMD. *See* ID at 33 ¶¶ 151, 153-54 (citing Wallace, Tr. at 1368-69, 1390-91 (“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.”)); *id.* ¶ 153 (citing Wallace, Tr. at 1370, 1383-84 (“The 1718 File was never found at any of the four IP addresses listed on CX0019.”)); *id.* ¶ 154 (citing Wallace, Tr. at 1443-44 (“To Mr. Wallace’s knowledge, the originating disclosing source in Atlanta is the only location at which the 1718 File was ever located.”)). As a result of the Wallace testimony as well as the OGR investigation into Tiversa and FTC, CC began advancing new theories of liability that have no basis in law or fact.

One such theory is based on a misreading of the Commission’s January 16, 2014 Order in this case. The FTC asserts that a “showing” of unreasonable security itself satisfies Section 5(n), because it asserts unreasonable security practices cause or are likely to cause substantial consumer injury. *See* CCOB at 24 n. 9. *But see id.* at 21 n.8 (“Of course, this does not mean that the ‘significant risk of harm’ standard is boundless.”). This theory appears to be a form of *per se* or strict liability. *See supra* Section II.A.3.b. It is factually and legally erroneous.

In *Resnick v. Av-Med, Inc.*, unencrypted laptops containing the sensitive information of approximately 1.2 million consumers were stolen and then sold “to an individual with a history of dealing in stolen property.”<sup>8</sup> 693 F.3d 1317, 1322 (11th Cir. 2012). The plaintiffs alleged they were “victims of identity theft and [had] suffered monetary damages as a result.” They also alleged that their health information was disclosed without authorization and this constituted negligence *per se* under Florida law. *Id.* at 1323, 1329. The Court stated:

Plaintiffs contend that they are a part of the class of people the statute sought to protect and that the harm they suffered was the type of harm the statute sought to avoid, thereby concluding that AvMed was negligent *per se*. . . . [But the Florida law] does not purport to regulate AvMed’s behavior, and so AvMed’s failure to comply with the statute cannot serve as a basis for a negligence *per se* claim.

*Id.* at 1328-29. Like the medical confidentiality statute<sup>9</sup> in *Resnick*, Section 5(n) did not regulate LabMD medical data security in 2007-2008. HIPAA did. And the FTC has not alleged any violation of HIPAA in this case. *See* Compl. ¶¶ 1-23.

---

<sup>8</sup> The FTC assertion that the Sacramento documents were found in the hands of “known identity thieves” is as inaccurate now as its claim in the past that the 1718 File was found “in ‘multiple locations’ on peer-to-peer networks, including at IP addresses belonging to suspected or known identity thieves[.]” *Id.* at 60, 75. Neither claim was ever proven by CC.

<sup>9</sup> Fla. Stat. § 395.3025 (2009).

Moreover, under Section 5(n) *per se* or strict liability applied to medical data security cases requires proof by a preponderance of reliable, probative, and substantial evidence that the LabMD acts or practices caused injury or are likely to cause substantial injury. “[T]he 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.” ID at 55 (note omitted). Unlike *Resnick*, where the unencrypted stolen laptops were sold to a known identity thief, the FTC has not alleged facts which would allow a reasonable trier of fact to conclude that there is any probability of likelihood of substantial injury. This is what Section 5(n) requires. *See Resnick*, 693 F.2d at 1322. The 1718 File was stolen by Tiversa, and then handed over to FTC and Eric Johnson, none of whom are within the group that Congress protected when it enacted HIPAA and HITECH.

Another variation of the FTC theory of *per se* or strict liability is that under Section 5(n) “significant risk of concrete harm” without more equals substantial injury. *See* CCOB at 12 (“Indeed, the Unfairness Statement does not equate ‘significant risk of concrete harm’ as being ‘likely’ to cause injury; it states that ‘significant risk of harm’ is substantial injury in itself.”). Section 5(n) does not mention “significant risk of concrete harm,” nor does apposite case law support this position.<sup>10</sup>

Analysis of the PNO (which is unlawful) is helpful on this point. The PNO is not equitable but punitive and/or prospectively injunctive in nature; the FTC is not authorized to issue it. *See Heater v. FTC*, 503 F.2d 321, 322-327 (9th Cir. 1974). The fencing-in relief sought by the FTC is both unnecessary and unlawfully punitive in this case. *See Riordan v. SEC*, 627

---

<sup>10</sup> LabMD also incorporates this argument in response to the FTC legally erroneous assertions regarding actual injury, likelihood of future substantial injury, and Article III standing. *See* CCOB at 11, 21-22.

F.3d 1230, 1234 (D.C. Cir. 2010). Violations of the PNO under 15 U.S.C. § 45(l) would purportedly allow the FTC to seek “mandatory injunctions and such other and further equitable relief as they deem appropriate.” Therefore, the requested relief in the PNO comes within the ambit of case law examining proof of causation and injury under principles of prospective injunctive relief and Article III standing.

In *Focus on the Family v. Pinellas Suncoast Transit Authority*, the Circuit cited Supreme Court precedent that a plaintiff must have suffered a “concrete” injury that is demonstrably caused by the conduct complained of. 344 F.3d 1263, 1273 (11th Cir. 2003) (citing *Nat’l Parks Conservation Ass’n v. Norton*, 324 F.3d 1229, 1241 (11th Cir. 2003)); accord *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). And “where a plaintiff seeks prospective injunctive relief, it must demonstrate a ‘real and immediate threat’ of future injury in order to satisfy the ‘injury in fact’ requirement.” *Norton*, 324 F.3d at 1241 (citing *City of Los Angeles v. Lyons*, 461 U.S. 95, 103-04 (1983); *Wooden v. Bd. of Regents*, 247 F.3d 1262, 1283-84 (11th Cir. 2001)). Additionally, the requirement that an injury be directly “traceable” to alleged wrongful conduct is “something less than the concept of ‘proximate cause.’” *Focus on the Family*, 344 F.3d at 1273 (citing *Loggerhead Turtle v. City Council*, 148 F.3d 1231, 1251 n.23 (11th Cir. 1998)).

In criticizing the findings of the Chief ALJ regarding likelihood of future substantial injury, the FTC confuses the “directly traceable” standard (under a pre-trial Article III standing challenge) with the applicable burden of proof at trial which requires proof of proximate cause and injury by a preponderance of the evidence pursuant to Section 5(n). See CCOB at 7, 18. Under Section 5(n), the FTC must prove that the LabMD medical data security acts or practices as alleged caused or are likely to cause substantial injury. This requires proof by a preponderance of the evidence of both proximate causation and injury. By contrast, the FTC

argues it need not prove either causation (proximate or otherwise), or injury past, present, or future. *Id.* at 18. There are no “victimized consumer[s]” in this case. *Id.* The FTC confuses an issue of pleading with a requirement of proof, which it has not met.

The Initial Decision applied the correct standard of causation and injury under Section 5(n). The FTC did not proffer any evidence that the LabMD medical data security acts or practices in 2007-2008 were either “directly traceable” to any injury or likely substantial injury, or that the acts or practice proximately caused injury or are likely to cause injury. “Possible” injury does not mean probable or likely substantial injury pursuant to Section 5(n). *See* ID at 1-92; *Smith v. Triad of Alabama, LLC*, No. 14-324, 2015 U.S. Dist. LEXIS 132514, at \*14-31 (M.D. Ala. Sept. 2, 2015); *see also Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (“[W]e have repeatedly reiterated that ‘threatened injury must be *certainly impending* to constitute injury in fact,’ and that ‘[a]llegations of *possible* future injury’ are not sufficient.”) (citations omitted); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44-46 (3rd Cir. 2011); *In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28-33 (D.D.C. 2014).

(c) The Complaint Counsel argument regarding “law of the case” fails

During closing argument on September 16, 2015, and again in its opening brief, the FTC argued that the Commission’s January 16, 2014 ruling on the LabMD November 2013 motion to dismiss is the “law of the case” and that Chief ALJ Chappell’s putative disregard of this ruling is a “fatal flaw” requiring reversal of the Initial Decision. *See* Tr. at 56-62 (Sept. 16, 2015 – FTC Closing Argument); CCOB at 5-6, 24 n.9.

MS. VANDRUFF:

With respect to the consumer injuries, first, LabMD’s practices resulted in . . . a disclosure that constitutes a cognizable injury under section 5 in and of itself. . . .

Mr. Wallace's testimony raised serious questions about [our] evidence, and we're not relying on evidence of spread or on expert calculations related to that evidence to meet our burden.

But it's the law of the case that we do not need to make such a showing for Your Honor to find LabMD liable.

JUDGE CHAPPELL: Excuse me. Law of the case?

MS. VANDRUFF: Yes, Your Honor.

JUDGE CHAPPELL: How's that?

MS. VANDRUFF: Well, the commission held in this case that actual exposure of consumers' sensitive personal information is not necessary for section 5 liability.

JUDGE CHAPPELL: Prior to trial.

MS. VANDRUFF: Correct, Your Honor.

JUDGE CHAPPELL: It becomes law of the case, in your opinion.

MS. VANDRUFF: Your Honor, that that -- that --

JUDGE CHAPPELL: A ruling on a motion to dismiss becomes law of the case?

MS. VANDRUFF: In describing the standard --

JUDGE CHAPPELL: Did I get that right?

MS. VANDRUFF: Your Honor, the commission's opinion describing section 5 and its application is law of the case in this matter, correct, Your Honor.

JUDGE CHAPPELL: But you haven't cited any Court of Appeals case that agrees with that, have you?

MS. VANDRUFF: With -- I want to make sure that I understand the question. . . .

JUDGE CHAPPELL: That actual exposure – that actual -- that evidence of a breach, a single breach, is sufficient to sustain a violation of section 5.

MS. VANDRUFF: Your Honor, we are relying on the commission’s opinion in this case, Your Honor, for that proposition.

JUDGE CHAPPELL: All right. That’s what I wanted to make sure of. Go ahead. . . . And again, I’m going to give you another opportunity to cite any authority to me other than that opinion that that’s the law of the case, as you say. . . . I’m asking you to cite any authority to me, any case law, other than the ruling on A motion to dismiss in this case, that says a mere breach is sufficient harm to sustain a violation of section 5.

MS. VANDRUFF: Well, Your Honor, in *Accusearch*, a case heard by the District of Wyoming, the court -- and I just want to make sure that I find this citation for Your Honor. . . .

FTC CA at 56-58 (emphasis added).

This exchange demonstrates three points, all of which are erroneous as a matter of law. First, the FTC position is that disclosure of sensitive information in and of itself, without more, is sufficient to show actual harm or likelihood of substantial harm under Section 5(n). *See supra* Section II.A.4.a-b. Second, the FTC contends that the Commission’s January 16, 2014 ruling is “law of the case,” “controlling,” and Chief ALJ Chappell committed “clear legal error” by purportedly disregarding a pre-trial ruling denying a motion to dismiss. Third, the FTC has cited no case law or other authority to support the argument that the pre-trial ruling of the Commission was in any way precedential or binding on Chief ALJ Chappell or on the Eleventh Circuit.

The *Accusearch* decision is inapposite; it does not mention “law of the case” principles. As well, the Chief ALJ correctly stated that *Accusearch* involved actual harm. *See* CA at 62;

*FTC v. Accusearch, Inc.*, No. 06-105, 2007 U.S. Dist. LEXIS 74905 at \*23 (D.Wyo. Sept. 28, 2007) (“FTC has documented economic harm experienced by consumers whose phone records have been disclosed, including actual costs associated with changing telephone carriers and addressing necessary upgrades to the security of the accounts.”).

- (i) The “law of the case” doctrine: the FTC cannot rely on a pre-trial, non-merits decision of the Commission as controlling

“Under the law of the case doctrine, both the district court and the appellate court are generally bound by a prior appellate decision of the same case.” *Oladeinde v. City of Birmingham*, 230 F.3d 1275, 1288 (11th Cir. 2000) (citing *Venn v. St. Paul Fire & Marine Ins. Co.*, 99 F.3d 1058, 1063 (11th Cir. 1996)). “[T]he doctrine ‘directs a court’s discretion, it does not limit the tribunal’s power.’” *Murphy v. Federal Deposit Ins. Corp.*, 208 F.3d 959, 966 (11th Cir. 2000) (citing *Arizona v. California*, 460 U.S. 605, 618 (1983)). The Commission stated the MTD was decided utilizing Fed. R. Civ. P. 12(b)(6), which was a preliminary ruling on the adequacy of the FTC Complaint. *See* MTD Order at 3 (“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.) (citation omitted); *see also* *Vintilla v. United States*, 931 F.2d 1444, 1447 (11th Cir. 1991); *Villeda Aldana v. Del Monte Fresh Produce N.A., Inc.*, 578 F.3d 1283, 1288-89 (11th Cir. 2009); *accord* *Perez-Ruiz v. Crespo-Guillen*, 25 F.3d 40, 42 (1st Cir. 1994) (“Interlocutory orders, including denials of motions to dismiss, remain open to trial court reconsideration, and do not constitute the law of the case.”). This was not a ruling on the merits.

Additionally, “the law of the case doctrine does not apply to bar reconsideration of an issue when (1) a subsequent trial produces substantially different evidence, (2) controlling authority has since made a contrary decision of law applicable to that issue, or (3) the prior decision was clearly erroneous and would work manifest injustice.” *United States v. Robinson*,

690 F.2d 869, 872 (11th Cir. 1982) (citation omitted); *Riley v. Camp*, 130 F.3d 958, 988-89 (11th Cir. 1997).

A review of the Record in this case demonstrates that elements one and two under *Robinson* are applicable, which is all that is required. Having first filed its appeal in federal district court in Georgia, LabMD appealed the Commission's January 16, 2014 ruling to the Eleventh Circuit on May 14, 2014. After briefing and oral argument, the Court issued its opinion on January 20, 2015.

The Eleventh Circuit ruled that the Commission's January 16, 2015 Order was not a final order because it was not the "consummation of the agency's decisionmaking process." *LabMD, Inc. v. Fed. Trade Comm'n*, 776 F.3d 1275, 1278 (11th Cir. 2015) (citing *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997)). "By definition, the denial of a motion to dismiss ensures that the proceeding will continue to a later, final order. In the same way, a complaint is just an initial document." *Id.*

Moreover, because it is not a merits ruling, "no 'direct and appreciable legal consequences' flowed from [the Commission's Order], and 'no rights or obligations have been determined,' because the agency proceeding is ongoing." *Id.* (quoting *Bennett*, 520 U.S. at 178). FTC indeed argued that the January 16 Order was in no way final.

In fact, the FTC made the same argument before the Eleventh Circuit as it is making now, namely, the Commission's January 16, 2014 Order is a "definitive interpretation of the application of Section 5." *Id.* The Eleventh Circuit rejected the FTC argument on this point: ". . . we are not required to agree with the FTC's characterization of its own Order in the course of litigation. *Id.* (citing *Inv. Co. Inst. v. Camp*, 401 U.S. 617, 628 (1971); *William Bros. v. Pate*, 833 F.2d 261, 265 (11th Cir. 1987) ("[W]e do not agree that the [agency's] mere litigating

position is due to be given deference. . . . [T]he Supreme Court has on a number of occasions proscribed granting deference to a litigating position[.]”)).

Therefore, the second *Robinson* factor is met; and the FTC position is erroneous as a matter of law. LabMD also posits that the first *Robinson* factor is met because the administrative trial in this case produced “substantially different evidence” since the Commission’s Order in January 2014. The FTC has disavowed all of the Boback testimony. *See* ID at 10 (“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.’”) (citations omitted). The FTC has also disavowed all of the Tiversa evidence at issue, including but not limited to the “spread” of the 1718 File.<sup>11</sup> *Id.* at 10-11 (“[CC] further explained its retreat from Tiversa-provided evidence in its Post-Trial Brief, stating: ‘The assertions made on page 49 of [CC’s] pre-trial brief are not repeated here. [CC’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.’”) (citing [CC’s] Post-Trial Br. at 61 n.3). The “substantially different” Wallace testimony combined with an absence of preponderance of credible evidence establishing either actual harm or likelihood of substantial harm satisfies the first *Robinson* factor.

4. As a matter of law, CC failed to prove its theoretical case which was based on an *ad hoc* standard of unreasonableness

The FTC at all times bears the burden of proving all allegations in its Complaint by a preponderance of “reliable, probative, and substantial evidence.” 5 U.S.C. § 556(d).

---

<sup>11</sup> However, Chief ALJ Chappell found that CC had not in fact disavowed the Boback testimony or the Tiversa evidence. *See* ID at 10-11.

Commission Rule 3.51(c)(1) provides that “[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.” *See also* ID at 12 (citing *In re Chi. Bridge & Iron Co.*, No. 9300, 2005 FTC LEXIS 215, at \*3 n.4 (F.T.C. Jan. 6, 2005).

The FTC Brief argues that Chief ALJ Chappell committed a “fatal flaw” by failing “to analyze LabMD’s security practices before ruling that the practices were unlikely to cause substantial consumer injury.” CCOB at 24 n.9 (citing ID at 13). This argument fails because (1) Congress did not designate a standard regarding unreasonable medical data security practices under Section 5(n) for the time period 2007-2008; (2) Congress did not delegate to FTC the ability to create or alter the standard of proof by attaching an *ipse dixit* standard of unreasonableness onto Section 5(n); (3) the FTC did not issue a rule or regulation concerning this issue for the relevant time period; and, (4) per Section 5(n), the FTC must prove by a preponderance of the evidence actual harm or likelihood of substantial harm to prevail under Section 5(n).

Even assuming the LabMD data security practices were unreasonable in 2007-2008 (which they were not), the Commission has no authority under Section 5(n) to declare LabMD practices unlawful unless the FTC proves by a preponderance of the evidence those practices caused or are likely to cause substantial injury to consumers.<sup>12</sup> The FTC failed to do so.

---

<sup>12</sup> While the FTC argues otherwise, it also failed to prove the second and third prongs of the Section 5(n) test, that such actual harm or likely substantial harm “is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” Chief ALJ Chappell did not consider the second and third prongs of Section 5(n)’s standard of proof because the FTC failed to prove the first prong. *See* ID at 13-14; *see also id.* at 55-56.

The FTC also argues that Section 5(n) does not require proof of known identity theft. *See* CCOB at 17-19. This argument also fails: (1) the FTC wrongly relied on its “law of the case” argument to support its theory that “significant risk of concrete harm” is embodied in Section 5(n); (2) the FTC argues that the individuals in the 1718 File were not “notified” by LabMD of any disclosure, despite the fact that LabMD was not required to do so under HIPAA or HITECH; and, (3) the FTC has not proved by a preponderance of the evidence that the LabMD medical data security “act or practice cause[d] or is likely to cause substantial injury *at the time of the unfair conduct.*” CCOB at 18 (citing *Int’l Harvester Co.*, 1984 FTC LEXIS 2, at \*252 n.52). The time of the asserted “unfair conduct” was June 2007 to May 2008: the FTC has not proved injury or likelihood of substantial injury for that time period or following. The FTC citation to *International Harvester* betrays its argument. That case involved severe injury and death. *See* 1984 FTC LEXIS 2, at \*178-79 ¶ 276 (“As a result of fuel geysering some operators of such IH tractors were severely burned and one or more operators have been killed[.]”) (citation omitted).

- (a) The FTC assertion that ‘unreasonableness’ *in vacuo* suffices to prove a Section 5(n) violation is erroneous as a matter of law

CC urges the Commission to adopt an unlawful standard of proof<sup>13</sup> under Section 5(n) when it argues that “[a] showing of unreasonable security *itself* satisfies Section 5(n) because unreasonable security practices cause or are likely to cause substantial consumer injury that is not outweighed by the benefits to consumers or competition and is not reasonably avoidable by consumers.” CCOB at 24 n.9. This theory is linked to the “possibility” standard that Chief ALJ Chappell found insufficient. *See* ID at 14.

---

<sup>13</sup> The FTC here appears to be arguing some combination of negligence *per se* and strict liability, as a standard of care. Both fail as a matter of law. The FTC argument violates the express terms of Section 5(n) regarding the burden of proof necessary for the Commission to declare a data security act or practice unfair.

Demonstrating that something is “possible” does not, and cannot, satisfy the FTC burdens of proof and persuasion pursuant to Section 5(n). *See* ID at 87, 91-92 ¶¶ 32-37 (Conclusions of Law). Moreover, the FTC offered no evidence that the LabMD medical data security was “unreasonable” for the period June 2007 to May 2008. The FTC offered no evidence that the LabMD medical data security practices as alleged in 2007-2008 or at any time are likely to reoccur or likely to cause any substantial injury. All of the testimony of future risk, including expert testimony, talk in terms of possibility and is based on the false claim that the 1718 File was available on peer-to-peer networks in November 2013. (RX 525 (Kaufman, Dep. at 62 (“Well, certainly as of November 2013 the 1,718 file was still available on peer-to-peer networks.”))).

- (b) No basis in law exists for the FTC argument that “significant risk of concrete harm” is equivalent to likelihood of substantial injury under Section 5(n)

The CC argument that “significant risk of concrete harm” is equivalent to likelihood of substantial harm under Section 5(n) is erroneous as a matter of law. *See* CCOB at 17-18.

Congress did not include “significant risk of concrete harm” in the text of Section 5(n). Congress was no doubt well aware of the FTC desire to expand its administrative reach under the amendment, but Congress chose instead to limit FTC power/discretion as to what constitutes unfair practices. Congress did this by the requiring that the FTC prove by a preponderance of the evidence that a given act or practice actually caused injury or is likely to cause substantial injury.

“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.” ID at 54-55. CC does not address this finding.

Instead the FTC analysis focuses on “substantial harm” to the exclusion of likelihood or probability. *See* CCOB at 11-12. “Significant risk of concrete harm” cannot be “substantial injury” in and of itself: Section 5(n) and apposite case law require that substantial injury must be likely to occur under the facts of this case. *See FDIC v. Meyer*, 510 U.S. 471, 476 (1994); *see also Southwest Sunsites v. Fed. Trade Comm’n*, 785 F.2d 1431, 1436 (9th Cir. 1986); *Reilly*, 664 F.3d at 44-46.

“In data breach cases where no misuse is alleged . . . there has been no injury – indeed, no change in the status quo. Here, [the 1718 File medical records] are exactly the same today as they would have been had [LabMD’s workstation] never been hacked. Moreover, there is no quantifiable risk of damage in the future. Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker.” *Reilly*, 664 F.3d at 45 (citation omitted).

5. FTC theories of “exposure” and/or “disclosure” as proof that the LabMD medical data acts or practices in 2007-2008 caused injury or are likely to cause substantial injury pursuant to Section 5(n) are erroneous.

The FTC approach disregards the amendment of the FTC Act to include the standard of proof contained in Section 5(n). Moreover, the FTC “exposure is the harm”<sup>14</sup> and/or “disclosure is the harm”<sup>15</sup> theory of liability does not fit this case because the facts demonstrate that the group to which the 1718 File was disclosed after it was stolen – Tiversa, Eric Johnson, and FTC – are not in the class of individuals or entities (identity thieves) that 5(n) was drafted to thwart.

---

<sup>14</sup> “Exposure” of the 1718 File on Limewire from June 2007 to May 2008. *See* CCOB at 8-11, 23, 25-26, 34, 38-41.

<sup>15</sup> “Disclosure” of the 1718 File “to unauthorized parties.” *See* CCOB at 9, 11, 23, 25 n.10, 26, 28-29, 37-38, 40-41. However, the evidence demonstrates that the 1718 File was never “disclosed” to any person or entity except for Tiversa/Boback/Wallace, Eric Johnson, and FTC. This means FTC includes itself as an “unauthorized party” in receipt of stolen PII and PHI under HIPAA.

For this reason, the disclosure in 2007-2008 cannot rationally be used to indicate a probability or likelihood of substantial harm.

The “possibility” of some unknown future “risk” of concrete harm cannot satisfy the FTC burden of proof under Section 5(n). *See* ID at 54, 87-88; *see also id.* at 90 ¶¶ 22-23 (“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. 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.”) (numeration omitted).

“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.” ID at 54; *see also Fed. Trade Comm’n v. Dinamica Financiera LLC*, No. 09-03554, 2010 U.S. Dist. LEXIS 88000, at \*28 (C.D. Cal. Aug. 19, 2010) (“To establish that representations were likely to mislead, the FTC must show probable deception[.]”) (citation omitted).

The FTC has not pointed to any case in which likely substantial harm was proven; it has only pointed to cases where actual harm occurs. *See* ID at 53; CCOB at 1-42. “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.” *Id.* at 52 (relying on *Orkin Exterminating Co. v. Fed. Trade Comm’n*, 849 F.2d 1354, 1365 (11th Cir. 1988), *cert. denied*, 488 U.S. 1041 (1989) (finding of substantial injury based on undisputed

evidence that 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).

6. The FTC arguments regarding the Section 5(n) standard of proof for likelihood of substantial injury fail as a matter of law

The FTC misstates the issue when it argues that Chief ALJ Chappell erred by “requiring Complaint Counsel to present expert testimony quantifying [“with mathematical precision”] the probability that consumers will suffer injury as a result of LabMD’s data security failures.” CCOB at 19 (citing ID at 83-84). In fact the Chief ALJ held the FTC to minimal requirements under Section 5(n) that some evidence of likelihood of substantial harm must exist. Otherwise, the expert testimony of Kam and Van Dyke is “divorced from any measure of the probability’ that a data breach, and resulting identity theft harm, will occur in this case.” ID at 84 (citing *Int'l Harvester*, 1984 LEXIS FTC 2, at \*253 n. 52).

The FTC failure to adduce preponderant evidence of likely substantial harm is also caused by its reliance on the tainted and false evidence from Boback and Tiversa regarding the 1718 File. *See* RX0644 (OGR Report at 5-6). All of the FTC evidence is the direct “fruit” of the 1718 File. *See* Sheer Tr. 31; *see also* Wallace Tr. 1344, 1353, 1362-70; RX 541 (Boback, Dep. at 36-42); CX 0703 (Boback, Dep. at 142-143); RX 525 (Kaufman, Dep. at 20); *see generally* 42 U.S.C. § 1320d-6; Ga. Code Ann. § 16-9-93(a)-(c). Consequently, CX 0307, the 1718 File, and all derivative evidence – that is, the FTC’s entire case – is based on unreliable, if not false, evidence.

The FTC was forced to disavow this evidence, and in turn failed to prove likelihood of substantial harm. *See* ID at 10-11; *see also* CA at 56-57 (MS. VAN DRUFF: “When we stood before Your Honor in May of 2014, we intended to present evidence that the 1718 File had

spread on P2P networks, an issue that Your Honor previewed in a question from the bench moments ago. As we've described in our briefing, however, Mr. Wallace's testimony raised serious questions about that evidence, and we're not relying on evidence of spread or on expert calculations related to that evidence to meet our burden.""). Additionally, the FTC did not elicit any expert opinions regarding the probability of likely harm in the future. Such testimony is necessary to prove likelihood of substantial injury, but it is absent from the FTC case.

7. The FTC failed to prove by preponderant evidence that the alleged LabMD medical data security acts or practices from June 2007 to May 2008 caused injury or are likely to cause substantial injury as a causative consequence of the Sacramento Incident

The FTC failed to prove by a preponderance of the evidence that the LabMD medical data security practices from June 2007 to May 2008, or at any other relevant time, caused injury or are likely to cause injury to consumers as a proximate cause of the exposure of the Sacramento Documents.

"First, Complaint Counsel has failed to prove that the Sacramento Documents were maintained on Respondent's computer network. 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." ID at 72 (citation omitted).

The FTC "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.'" ID at 73 (citing CA at 54 ("We have not presented evidence of how those documents left the possession of LabMD"). Accordingly, there is no causative chain of custody between the PII on the LabMD medical data security networks and the Sacramento documents.

In May 2014, the Northern District of Georgia recognized the unreliability of the Sacramento evidence prior to trial in this case. Judge Duffey 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. Fed. Trade Comm’n*, No. 14-810, 2014 U.S. Dist. LEXIS 65090, at \*3 n.2 (N.D. Ga. May 12, 2014).

Finally, Chief ALJ Chappell was correct as a matter of law to exclude CX0451<sup>16</sup> as unreliable and lacking foundation. Mr. Kevin Wilmer, an FTC investigator, used CLEAR to obtain information on the Sacramento “Day Sheets.” “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 . . . .” ID at 39 ¶ 214. CC provided Mr. Wilmer with an electronic copy of CX0085, “which he was told consisted of copies of the Sacramento Documents.” *Id.* ¶ 215 (citing Wilmer, Tr. 338-339).

“Mr. Wilmer concluded, but did not confirm, that the nine digit numbers in pages 5 through 44 of CX0085 represented Social Security numbers.” *Id.* at 40 ¶ 217 (citing Wilmer, Tr. 340). Mr. Wilmer was asked by CC to determine whether SSNs 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.” *Id.* ¶ 218 (citing Wilmer, Tr. 340-42).

---

<sup>16</sup> A document, marked by the FTC for identification as CX0451, as the results returned to Mr. Wilmer by Thompson Reuters in response to his CLEAR database query, to which Mr. Wilmer added certain color coding to differentiate various names. *See* Wilmer, Tr. 350, 359.

“Mr. Wilmer issued a ‘query’ to the CLEAR database [by copying] each number that he believed to be a [SSN] 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. *Id.* ¶ 219 (citing Wilmer, Tr. 342-45, 359-60). At trial, Mr. Wilmer “did 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.” *Id.* ¶ 222 (Wilmer, Tr. 358). “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.” *Id.* ¶ 224 (citing Wilmer, Tr. 365). “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.” *Id.* ¶ 222 (citing Wilmer, Tr. 358).

“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.” *Id.* ¶ 223 (Wilmer, Tr. 363-64). “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.” *Id.* ¶ 224 (Wilmer, Tr. 365).

“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.” ID at 41 ¶ 227 (citing

F. 217-226). Chief ALJ Chappell was correct as a matter of law to exclude CX0451 from evidence because it was unreliable and lacked a proper foundation. *See* ID at 70-80 (“ . . . 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.”) (emphasis original); (“ . . . 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, [CC] 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.’”); (“ . . . 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.”).

B. The Initial Decision Is Correct Per the Evidence Presented At The Hearing

1. Complaint Counsel failed to adduce qualified expert testimony as appropriate opinions necessary to prove that LabMD violated Section 5(n)

(a) Negligence standards as applied to Section 5(n)

The FTC asserts that common law negligence standards inform allegations of “unreasonable data security” in this case. *See* CCCL ¶ 16. LabMD also argued negligence concepts in defining what “reasonableness” may mean under Section 5(n). *See* ID at 85; *see also* RCL ¶ 97.

The analysis by Chief ALJ Chappell explains why the FTC failed to sustain its burden of proof required by Section 5(n) for the allegations in the Complaint. Contending “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.” ID at 86 (citing Compl. at ¶¶ 10, 22; *LabMD, Inc.* 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).

Additionally, “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.” *Id.* at 86 (citing H.R. CONF. REP. 103-617, 1994 WL 385368, at \*11-12, FTC Act Amendments of 1994 (commentary 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); 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)).

“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. 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.” ID at 87 (citation omitted); *see also* CCOB at 12, 24 n. 9.

- (b) FTC experts failed to offer reliable, probative, and substantial opinion evidence of actual harm or likelihood of substantial harm under Section 5(n)
  - (i) Expert testimony is required to prove unfairness under Section 5(n)

The FTC opening brief argues that the ID “incorrectly requires [CC] to present expert testimony quantifying the probability<sup>17</sup> that consumers will suffer injury as a result of LabMD’s data security failures.” *See* CCOB at 19 (citing ID at 83-84). The FTC assertion here is erroneous as a matter of law — the FTC is required to prove likely substantial injury, as opposed to the “possibility” of injury, and this is the standard addressed in the Initial Decision.

In order to carry its burden under Section 5(n), the FTC must adduce qualified expert testimony regarding the issue of whether the LabMD data security practices caused injury or are likely to cause substantial injury because this issue is generally one for specialized expert knowledge beyond the ken of the average layperson or factfinder. *See Zwiren v. Thompson*, 578 S.E.2d 862, 865 (Ga. 2003). In the tort context, proximate causation includes all of the natural and probable consequences of the tortfeasor’s negligence, unless there is a sufficient and independent intervening cause.<sup>18</sup> *See Blakely v. Johnson*, 140 S.E.2d 857, 859 (Ga. 1965) (imaginary or remote damages are not actionable).

---

<sup>17</sup> The FTC brief implies throughout that “possibility” and “probability” are equivalent and interchangeable terms. This is wrong as a matter of law — these words mean different things in the context of the burden of proof under Section 5(n). These semantic juxtapositions underscore the FTC failures of proof as a matter of fact and law.

<sup>18</sup> Absent the Tiversa crime (theft of the 1718 File from LabMD), and its false evidence (fraudulently claiming “spread” of the 1718 File on the P2P network), there is no case against LabMD. *See* CA at 48-50 (JUDGE CHAPPELL: “All right. You’re refusing to answer my question. Move along.” MS. VANDRUFF: “No, I’m not.” JUDGE CHAPPELL: “I’ve given you four or five opportunities, Counselor. It’s yes or no. You keep wanting to push your agenda here, and I’m fine with that, that you’re an advocate for your client. I understand that. But if you never had the 1718 File, there wouldn’t have been an investigation of LabMD; correct?” MS.

An opinion of an expert must be within a reasonable degree of certainty or probability. *Zwiren*, 578 S.E.2d at 865-68 (expert testimony must provide a causal connection that is more than mere chance, possibility or speculation that the alleged negligent act(s) cause or are likely to cause substantial harm to a consumer); Partial Dissent of Comm’r Maureen K. Ohlhausen at 7, *In re ECM BioFilms, Inc.*, No. 9358 (F.T.C. Oct. 19, 2015).

Likelihood is synonymous with probability. See *In re Terazosin Hydrochloride Antitrust Litig.*, 352 F. Supp. 2d 1279, 1300-01 (S.D. Fla. 2005) (the word “likelihood” is synonymous with “probability”) (citing *Shatel Corp. v. Mao Ta Lumber & Yacht Corp.*, 697 F.2d 1352, 1356 n.2 (11th Cir. 1983)).

“[I]n defining the word ‘probability,’ the Eleventh Circuit has recognized that it is capable of two definitions: a lower ‘reasonable probability’ standard, or a higher ‘more likely than not’ standard.” *Terazosin*, 352 F. Supp. at 1301 (citations omitted). “But ultimately, the definition most often applied in [Eleventh Circuit] precedent is the ‘more likely than not’ standard.” *Id.* (citing *Mercantile Tex. Corp. v. Bd. of Governors of Fed. Reserve Sys.*, 638 F.2d 1255, 1268 (5th Cir. 1981)); cf. *United States v. Marine Bancorporation, Inc.*, 418 U.S. 602, 622-23 (1974) (§ 7 of the Clayton Act (15 U.S.C. § 18) “deals in ‘probabilities,’ not ‘ephemeral possibilities’”) (quoting *Brown Shoe Co. v. United States*, 370 U.S. 294, 323 (1962))). In either instance, the expert testimony proffered by CC falls short of what is required in this matter.

Complaint Counsel introduced testimony from three expert witnesses<sup>19</sup> and one

---

VANDRUFF: “It may be the case that without having learned of the disclosure –” JUDGE CHAPPELL: “At least we wouldn’t be here today, this hearing, this whole procedure wouldn’t have happened; correct?” MS. VANDRUFF: “I can’t know that, Your Honor. . . .”

<sup>19</sup> Raquel Hill, Rick Kam, and Jim Van Dyke.

rebuttal expert<sup>20</sup> to prove its case and satisfy its burden. When ruling on expert opinions, “courts consider whether the expert is qualified in the relevant field and examine the methodology the expert used in reaching the conclusions at issue.” *McWane, Inc.*, 2012 FTC LEXIS 142, at \*8 (citations omitted); *see also* RPCOL at 43 ¶ 164.

A party proffering expert opinion evidence bears the burden of establishing its admissibility. *See Pride v. BIC Corp.*, 218 F.3d 566, 578 (6th Cir. 2000). The ALJ must act as a gatekeeper, admitting only that expert testimony which is relevant and reliable. *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 589 (1993). For an expert opinion to be relevant “there must be a ‘fit’ between the inquiry in the case and the testimony.” *United States v. Bonds*, 12 F.3d 540, 555 (6th Cir. 1993). For an expert opinion to be reliable, *Daubert* requires the trier of fact to evaluate: (1) whether the analytic technique or opinion has been subjected to peer review or publication, (2) the “known or potential rate of error,” (3) a “reliability assessment,” in which the “degree of acceptance” within a scientific community may be determined and reviewed, and (4) the “testability” of the opinion. *See Daubert*, 509 U.S. at 592-94; *see RCL* at 39 ¶¶ 149-52.

“A witness who invokes ‘my expertise’ rather than analytic strategies widely used by specialists is not an expert as Rule 702 defines that term.” *Zenith Elecs. Corp. v. WH-TV Broad. Corp.*, 395 F.3d 416, 419 (7th Cir. 2005). Nothing requires a court to admit opinion evidence which is connected to existing data only by the *ipse dixit* of the expert. *See Gen. Electric v. Joiner*, 522 U.S. 136, 146 (1997). Additionally, the party presenting the expert must show that the expert findings are based on sound reasoning, and this will require some objective,

---

<sup>20</sup> Clay Shields.

independent validation of the expert's methodology. *Daubert v. Merrell Dow Pharms.*, 43 F.3d 1311, 1316 (9th Cir. 1995).

- (c) FTC expert Raquel Hill<sup>21</sup> failed to provide reliable, probative, and substantial opinion evidence of actual injury or likelihood of substantial injury under Section 5(n)
  - (i) Dr. Hill failed to apply her opinion to the June 2007 to May 2008 time frame

Dr. Hill 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)). *See* RFF at 86 ¶ 359. 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. at 307-309). *Id.* at ¶ 360; (citing CX 0740 (Hill, Exp. Rep. at 13-15)).

Dr. Hill did not proffer any opinions in this case within a reasonable degree of likelihood or probability.

Dr. Hill was unaware of any document that cites all of her “seven principles for a comprehensive information security program.” RFF at 86 ¶ 362 (citing Hill, at Tr. 242-43). Most importantly, LabMD cannot be held to this “standard” because it was not established that such standard existed and was applicable to LabMD for the relevant time period. Moreover, Dr.

---

<sup>21</sup> Dr. Hill admits that portions of her report follow closely along with the allegations contained in paragraph 10 of the Complaint. *See* RX 524 (Hill, Dep. at 58); RFF at 73 ¶ 314. Dr. Hill’s opinions were limited to the “relevant time period,” which at that time was January 2005 through and including July 2010. *See* ID at 87 n.45. The FTC opening brief now asserts that LabMD’s allegedly unreasonable data security practices are limited to an eleven month period in 2007-2008. *See* CCOB at 4, 8.

Hill only became aware of the so-called defense-in-depth strategy circa mid-2009. *Id.* at ¶ 365 (citing Hill, Tr. 306).

There is no perfect data security. RX0524 (Hill, Dep. at 149); Commission Order Denying Respondent LabMD’s Motion to Dismiss, at 18 (Jan. 16, 2014) (citation omitted). 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’s November 2011 “guide”<sup>22</sup> regarding data security standards, or in what standards may have been in place from June 2007 to May 2008. *See generally* Hill Tr. at 235-36.

An expert’s testimony must “fit” the case at hand. *See United States v. Bonds*, 12 F.3d 540, 555 (6th Cir. 1993). Dr. Hill’s opinion does not “fit” this case as a matter of law because she evaluated LabMD’s data security using broad, general IT principles from 2014, without reference to or apparent knowledge of medical industry standards and practices during 2007-2008. *See* Hill Tr. at 230-31, 234; RX0524 (Hill, Dep. at 61); RFF at 73-89 ¶¶ 331-385.

Dr. Hill “considered” only the HIPAA Security Rule. Hill, Tr. at 231. She did not consider the rest of the statutory or regulatory HIPAA/HITECH data security regime, or perform the “scalability” analysis HIPAA requires to differentiate between large and small medical providers. However, “scalability” is a key tenet of the HIPAA security standard, *see* HIPAA Security Series, Security 101 for Covered Entities at 1, 7 (Vol. 2 Paper 1) (11/2004: rev. 3/2007), which provided that data security compliance must be judged according to the size and nature of the medical provider in question. *See also* Health Insurance Reform: Security Standards, 68 Fed.

---

<sup>22</sup> The FTC “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, and three to four years after the relevant time period of June 2007 to May 2008. *See* ID at 32 ¶ 90.

Reg. 8334, 8338-49, 8351, 8359-64, 8367-69, 8372-73 (Feb. 20, 2003); 45 C.F.R. Parts 160, 162, 164.

As the only FTC expert on “reasonable” data security, Dr. Hill failed to opine what data security standards were in place from June 2007 to May 2008, and how LabMD conduct fell short of meeting those standards. The FTC argument that LabMD had “multiple, systemic, and serious” flaws in its network security practices is not based upon any legal standard. The FTC did not prove what “reasonable” PHI data security was during 2007-2008, or at any other relevant time.

In summary, the FTC failed to adduce reliable, probative, and preponderant opinion evidence, based upon a reliable expert opinion to a reasonable degree of certainty or probability, that the LabMD data security practices in 2007-2008 as alleged were “unreasonable.” Dr. Hill also did not establish that such acts or practices caused or are likely to cause substantial injury.

The Commission is without authority to declare the LabMD alleged data security acts and practices unfair under Section 5(n).

(ii) Dr. Hill’s Report and Testimony

“Complaint Counsel’s proffered expert on computer security, Dr. Raquel Hill, 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 the LabMD 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)).” *See* ID at 42 ¶ 237. Dr. Hill’s opinion is inadequate. The CC failed in its burden of proof under Section 5(n).

Dr. Hill’s conclusions in this case were limited to the time period from January 2005 through July 2010. *See* ID at 16 ¶ 7. Dr. Hill also concluded that LabMD’s physical security was

adequate. *See* Hill, Tr. at 293; *see also* RFF at 75 ¶ 326 (citing RX0524 (Hill, Dep. at 118-119)). Dr. Hill did not opine on the CC allegations involving the Sacramento Day Sheets nor did she offer an opinion on actual harm or likely substantial harm to consumers. *See* Hill, Tr. at 218.

The Hill assumptions that (1) identity theft harm could occur if the information contained on LabMD’s network was exposed, and (2) in assuming such harm could occur, that such harm was likely, were clarified by Chief ALJ Chappell as follows:

JUDGE CHAPPELL: “Whoa, whoa, whoa. Wait a minute. Sorry to interrupt. If you assumed it could occur, does that not mean you assumed it was likely? Isn’t that the same thing?”

[Dr. Hill]: “I’m sorry, sir. I thought that he had said that it had –”

JUDGE CHAPPELL: “No, no, I’m not talking about what he said.”

[Dr. Hill]: “Oh, okay.”

JUDGE CHAPPELL: “I’m reading plain English here. Do you need her to read my question back?”

[Dr. Hill]: “Yes, sir.”

[The question was read back]

[Dr. Hill]: “Oh, that it was likely? Yes, sir.”

JUDGE CHAPPELL: “Thank you. Go ahead.”

BY MR. SHERMAN: “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?”

[Dr. Hill:] “I have no opinion, yes.”

*Id.*

As “[t]he only expert proffered by [CC] who [was] arguably qualified to assess the degree of risk posed by Respondent’s computer security practices, [Dr. 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.” ID at 84 (emphasis in original).

“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.” ID at 84-85.

CC never properly elicited an opinion from Dr. Hill, based upon a reasonable degree of certainty or probability, as to whether the LabMD’s data security practices in 2007-2008 or during the “relevant time period” actually caused or are likely to cause substantial injury to consumers. Moreover, Dr. Hill’s “standard of care” testimony was not within a reasonable degree of certainty or probability. The foundation for her opinion was a concept called “defense-in-depth” which was not in effect during 2007-2008 – in fact, Dr. Hill did not learn of such a standard herself until sometime around 2009. *See* Hill, Tr. at 306.

Therefore, Dr. Hill’s opinion on “unreasonableness” is inadmissible. *See generally* RFF at 73-89 ¶¶ 313-385.

(d) The Kam expert opinion is not reliable, probative, or substantial and the ID correctly ruled the opinion should be accorded little or no weight

(i) Rick Kam's report and testimony

“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. Mr. Kam was asked to ‘assess the risk of injury to consumers caused by the unauthorized disclosure of [consumers’] sensitive personal information.’” ID at 16 ¶¶ 9, 11.

Mr. Kam did not proffer any opinions in this case within a reasonable degree of likelihood or probability.

Mr. Kam's only educational degree is in management and marketing. *See* Kam, Tr. at 516. Mr. Kam has no expertise in computer network security. *Id.* at 518. His 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. *See* Kam, Tr. at 549-552; RX0522 (Kam, Dep.) at 44-49. In developing his personal four-factor methodology, Mr. Kam never used statistical analysis, apparently never spoke to data privacy professionals, and never allowed any review of his methodology because of confidentiality agreements in place. *See* Kam, Tr. at 549-52. This personally-developed methodology has never been published, peer reviewed, or reviewed in any form. *See* Kam, Tr. at 552.

Mr. Kam applied this four factor “risk assessment test” to determine the likelihood of harm from the theft of the 1718 File. *See* ID at 42 ¶ 239 (citing CX0742 (Kam Exp. Rep., at 18-19)).

Like Mr. Van Dyke,<sup>23</sup> “Mr. Kam ‘assumed that LabMD failed to provide reasonable and appropriate security for consumers’ personal information maintained on its computer networks.’” *See id.* at 43 ¶ 244 (CX0742 (Kam Exp. Rep. at 5)).

In applying the second and third factors of his four-factor test 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 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.” *See id.* at 42 ¶ 240 (citing CX0742 (Kam Exp. Rep., at 19); Kam, Tr. 409-410)). Mr. Kam also relied on Boback’s discredited testimony “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.” *Id.* ¶ 241 (citing CX0742 (Kam Exp. Rep. at 19); Kam, Tr. 409-410)).

Mr. Kam testified that in every data breach, some victim has come forward. *See* Kam Tr. at 532. However, Mr. Kam knew of no actual victims of identity theft or fraud of any individuals listed on the 1718 File. *See id.* at 533. In fact there were none.

Mr. Kam’s opinion regarding the likelihood of medical identity theft harm was based primarily on the 2013 Survey on Medical Identity Theft by the Ponemon Institute. *See* ID at 43 ¶ 246 (citing CX0742 (Kam Exp. Rep. at 15, 19-20); Kam, Tr. 423)). The 2013 Ponemon Survey was unreliable, non-probative, and non-substantive because it (1) had a response rate of only 1.8 %, which Mr. Kam agreed created a non-response bias; and (2) the sampling frame contained individuals who were prescreened from a larger sample on the basis of their identity

---

<sup>23</sup> *See infra* pp. II.B.1.e.

theft or identity fraud experience, which Mr. Kam agreed resulted in a sampling frame bias. *See id.* ¶¶ 247-48 (citing Kam, Tr. at 540-41); RX0528 (2013 Ponemon Survey, at 28, 31-32).

CC violated its representation to the Tribunal, and to LabMD Counsel, that “it would not rely on expert opinion based on the testimony of Mr. Boback or on CX0019.”<sup>24</sup> *See* ID at 61 (citing ID at 10-11 Section I.B.2.) (“On June 24, 2015, CC announced for the first time that it ‘does not intend to cite to [Boback’s] testimony or CX0019 in its proposed findings of fact. Nor does [CC] intend to cite to expert conclusions predicated on [Boback’s] testimony or CX0019.’ . . . However, as shown *infra*, [CC] does rely on expert opinions that were predicated on [Boback’s] testimony. In addition, [CC] relies on [Boback’s] deposition testimony to counter Respondent’s Proposed Findings of Fact. *See, e.g.*, CCRRFF 72b, 73b, 74b.”).

Significantly, applying the Kam four-factor “methodology” 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 [because] 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 [CC] where Personal Information was allegedly obtained by computer hackers and used to commit credit card fraud.” *See* ID at 61 (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 690-694 (7th Cir. 2015)).

---

<sup>24</sup> CX0019 is the fraudulent listing of four IP addresses on a plain piece of paper which Boback testified proved the “spread” of the 1718 File on the P2P network. *See* OGR Report at 3-78. All of Boback’s claims were inaccurate and all of the “evidence” that the 1718 File had “spread” was false.

Chief ALJ Chappell ruled that the Kam opinion regarding the 1718 File was entitled to no weight. *See id.* at 61.

- (e) The Van Dyke expert opinion is not reliable, probative, or substantial and it was correctly ruled the opinion should be accorded little or no weight
  - (i) The Van Dyke Report and Testimony

Jim Van Dyke is the founder and President of Javelin Strategy & Research. He was instructed by the 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.” (CX0741 (Van Dyke, Exp. Rep. at 2)). In rendering his opinion, Van Dyke assumed that “LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks.” (CX0741 (Van Dyke, Exp. Rep. at 2)). Specifically, 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. 678-79).

However, Mr. Van Dyke did not proffer any opinions in this case within a reasonable degree of likelihood or probability.

“Subjective methodology, as well as testimony that is insufficiently connected to the facts of the case, have been relied upon by appellate courts as grounds for rejection of expert testimony.” *Souther v. Eli Lilly & Co.*, 489 F. Supp. 2d 230, 284 (S.D.N.Y. 2007). “The Supreme Court has stressed that ‘nothing in either *Daubert* or the Federal Rules of Evidence requires a district court to admit opinion evidence that is connected to existing data only by the *ipse dixit* of the expert. A court may conclude that there is simply too great an analytical gap between the data and the opinion proffered.’” *Arista Records LLC v. Lime Group LLC*, 2011 U.S. Dist. LEXIS 47416, at \*12 (S.D.N.Y. Apr. 29, 2011) (citations omitted).

In this case, the Van Dyke analysis is disconnected from the facts of the case, which render his opinions unreliable. *See* RX0523 (Van Dyke Dep., at 39) (testifies that he “had[n]’t given any consideration” to how the insurance aging file was taken). The Van Dyke admission that he never considered any of the specific facts of the case, *id.* at 72-73, illustrates that the Van Dyke opinions are speculative and unreliable. *Cf. Brooks v. Outboard Marine Corp.*, 234 F.3d 89 (2nd Cir. 2000).

The Van Dyke report and opinions prior to trial relied on Boback’s false and unreliable November 2013 testimony. *See* ID at 7-8 (citing CX0741 (Van Dyke, Exp. Rep.at 7-8, 12-14); RX0523 (Van Dyke, Dep. at 42, 107-08). The Van Dyke opinions at trial regarding ongoing identity theft or medical identity theft also specifically relied upon Boback’s false and unreliable November 2013 testimony regarding the 1718 File and the Day Sheets. *See* Van Dyke, Tr. at 645-46.

Van Dyke is not a statistician, yet his report relied upon a “cross-tabulation” technique which involves “comparison of statistical data.” *See* Van Dyke, Tr. at 587, 673-75. The Van Dyke definition of “cross-tabulation” is confusing and inconsistent.

Van Dyke never surveyed anyone from the 1718 File for purposes of his report, opinion, and testimony in this case. *See* Van Dyke, Tr. at 677-78. Furthermore, Van Dyke did not account for the type of breach or who gained the information, and also 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. *See* RX0523 (Van Dyke, Dep. at 41-43).

As applied to this case, the Van Dyke expert projection that within one year of unauthorized disclosure, 7.1% of the individuals on the 1718 File list should have experienced

non-card identity fraud was erroneous because there were no victims of identity theft from the 1718 File. *See* Van Dyke, Tr. at 692.

Chief ALJ Chappell ruled that “the 2013 Javelin Survey, the 2014 Javelin Report, and the Van Dyke 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.” *See* ID at 64. This is so for several interconnected reasons.

“First, and perhaps most important, [CC’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.” *Id.* The CC failure to locate a single victim “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.” *Id.* (citing *In re McWane, Inc.*, No. 9351, 2013 FTC LEXIS 76, at \*730-31 (F.T.C. May 8, 2013)).

“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 [CC] 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.” *Id.*

at 65.

“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. . . . 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.” *Id.*

In summary, the Chief ALJ correctly decided that the opinion offered by Van Dyke “fail[ed] to assess the probability or likelihood that Respondent’s alleged unreasonable data security will result in a data breach and resulting harm.” *Id.* at 83.

2. The testimony of rebuttal expert Clay Shields does not cure the failure of Complaint Counsel to prove the LabMD medical data security practices, as alleged, caused injury or are likely to cause substantial injury

Having failed to adduce reliable, probative, and substantial preponderant expert testimony in its case-in-chief, the FTC argues that rebuttal expert Clay Shields did so. *See* CCOB at 32-34.

The FTC argues the Clay Shields testimony is reliable, probative, and substantial preponderant evidence of the asserted “heightened significant risk of concrete injury” standard under Section 5(n), which the FTC argues was created solely by the alleged LabMD sharing of patient files on the P2P Network. *See* CCOB at 32. The FTC also asserts that “[c]ontrary to the Initial Decision’s apparent conclusion that the 1718 File could be found only by someone who knew the exact file name, Dr. Shields’s unrebutted testimony established that there were at least

three relatively simple ways that P2P users, particularly malicious users, could have located the 1718 File without knowing the file name.” *Id.*

LabMD has detailed the problems associated with the asserted FTC standard of care, which appears nowhere within Section 5(n). The other significant problem with the FTC reasoning regarding Dr. Shields is there is no opinion of the probability of likely substantial harm within his testimony. *See* CX0738 (Shields, Rebuttal Exp. Rep. at 4-5, 31 ¶¶ 2, 31). CC argues that some unknown “malicious” entity or person “could have” located the 1718 File. For example, the FTC asserts that a “malicious user who found LabMD’s computer by searching for other terms would be especially likely to use browse host and examine any files that were likely to contain sensitive personal information, such as a file containing the term ‘insurance.’” *See* CCOB at 33. However, there is no evidence that any user, malicious or otherwise, used browse host to examine any LabMD file between June 2007 and May 2008, nor was there any such opinion. Such an examination requires downloading the file, and the only downloading of the 1718 File in this case was done by Tiversa. *See* ID at 60.

This underscores a critical point: a file which is “available for sharing” on P2P cannot satisfy the Section 5(n) burden of proof requiring injury or likelihood of substantial injury because the file must be downloaded for the file’s contents to be viewed. *See* ID at 23 ¶¶ 66-68 (“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. 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. The contents

of a file that is available for sharing are not disclosed until the file is downloaded and viewed.”) (citing Shields, Tr. at 891-92; Wallace, Tr. at 1343; F. 65-67).

There must be an intentional act whereby the file is downloaded and viewed for actual harm or likely substantial harm to even be considered. *Cf.* ID at 60, 65. *See generally* ID at 23-24 ¶¶ 65-77. There is no evidence that the 1718 File was ever downloaded and viewed by anyone other than Tiversa, *see id.* at 60, and downloading the 1718 File is the causative act that is essential before actual harm or likely substantial harm can be considered. The FTC failed to prove that identity thieves, or anyone save Tiversa, downloaded and viewed the 1718 File. The FTC case fails under Section 5(n).

- (a) The Clay Shields rebuttal testimony failed to offer an opinion that the LabMD medical data security practices in 2007-2008 caused or are likely to cause substantial harm to consumers

Dr. Clay Shields is CC’s rebuttal expert, who was asked to review the conclusions of LabMD’s expert, Mr. Adam Fisk. *See* CX0738 (Shields, Rebuttal Exp. Rep. ¶¶ 1-2)); ID at 17 ¶¶ 16, 19 (citation omitted). However, Dr. Shields did not proffer any opinions in this case within a reasonable degree of likelihood or probability.

The LabMD expert witness, Mr. Adam Fisk, “was asked to provide an opinion as to whether LabMD provided adequate security to secure Protected Health Information contained within its computer network from January 2005 through July 2010 (the “Relevant Time Period” assessed by Dr. Hill).” *Id.* at 18 ¶ 21. “Mr. Fisk is the former lead engineer at LimeWire LLC, the creators of the LimeWire file-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.” *Id.* at 17-18 ¶ 20 (citing RX0533 (Fisk Exp. Rep., at 3-4)). “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.” *Id.* at 18 ¶ 21 (citing RX0533 (Fisk Exp. Rep., at 3-4)). “Mr. Fisk based his opinions of the facts of this case on his extensive experience and documents provided to him by Respondent.” *Id.* ¶ 22 (citing RX0533 (Fisk Exp. Rep., at 3-4, 37)). “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.” *Id.* ¶ 22 (citing Fisk, Tr. 1158-1159).

“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.” *Id.* at 23 ¶ 65 (citing CX0738 (Shields Rebuttal Exp. Rep., ¶ 18)). “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.” *Id.* ¶ 66 (citing Shields, Tr. 891-892).

This last point regarding the difference between a file on P2P’s Gnutella network being “available for sharing” and “downloading” is critical because the FTC never proved the 1718 File was downloaded or “pull[ed] down” by anyone other than Richard Wallace and Tiversa. *See also* Wallace, Tr. at 1345 (Q. “So is it your testimony that while doing your job, you would search the peer-to-peer networks and pull down any and all information that was available?” A. “That is correct, yes.” Q. “You used the term ‘pull down.’ Does that mean that you would download those files?” A. “Yes.”).

To this point, the Chief ALJ correctly made the following findings:

- “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.”
- “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.”
- “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.”
- “[E]vidence, 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.”
- “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.”

ID at 60 (citations omitted). In its opening brief, the FTC did not dispute any of the foregoing findings by Chief ALJ Chappell.

The FTC attempts to strengthen its assertion that the “disclosure alone is the harm” is by its suggestion that the 1718 File was “available for sharing.” As a result, it argues Tiversa was able to download the file – the disclosure of PHI to Tiversa (and presumably Eric Johnson and FTC) is sufficient to demonstrate actual injury or likelihood of substantial injury. *See* CCOB at 40 (“The foregoing demonstrates the broad recognition of the inherent harm in the exposure of medical information. The exposure need not result in further injury – the mere disclosure is the harm.”); *cf.* CCOB at 24 n.9. This theory of *per se* or strict liability is not available under Section 5(n), and even if it were, the FTC cannot prove causation of injury or likely substantial injury.

There are other deficiencies in the FTC arguments on this point. The FTC did not proffer an expert witness with respect to P2P networks or LimeWire – Clay Shields testified as a rebuttal witness only. *See* Tr. 747-49. Additionally, Professor Shields has limited, if any, experience with LimeWire; he did not attempt to find the 1718 File on the Gnutella network as he wrote his rebuttal expert report or prepared to testify. *See* Shields, Tr. at 892-93. Professor Shields did not know how the LabMD 1718 File was “actually shared,” obtained by Tiversa, or if or how the 1718 File got on the network. *See* Shields, Tr. at 904-07.

Additionally, Professor Shields’ opinions were based on the discredited deposition of Boback, *see* Shields, Tr. at 904-06, and as a result he assumed that the 1718 File had been shared and made available over Gnutella on the LimeWire network.

Finally, in a metaphor for the FTC failures of proof under Section 5(n), Professor Shields acknowledged that finding one particular file on the Internet by use of LimeWire is akin to winning the lottery. *See* Shields, Tr. at 917.

3. Citations to Georgia privacy law do not prove by reliable, probative, and substantial preponderant evidence that the LabMD medical data security practices as alleged in 2007-2008 caused or are likely to cause substantial injury to consumers
  - (a) The FTC argument for Section 5(n) liability under theories of Georgia tort law fail

The FTC argues that Tivera's "unauthorized" downloading of the 1718 File caused those consumers harm by invading their right to privacy in their personal medical information under Georgia tort law. *See* CCOB at 39-41. This argument by analogy is but another form of the FTC position that there is "inherent harm in the exposure of medical information. The exposure need not result in further injury – the mere disclosure is the harm." *Id.* at 41. The actors in this latest version of the FTC theory of liability are Richard Wallace and Tiversa, who are now characterized by FTC as an "unauthorized third part[ies]." <sup>25</sup> *Id.* at 40. Therefore, the FTC argument is that the Richard Wallace and Tiversa<sup>26</sup> intentional theft of the 1718 File for private gain is somehow evidence that the LabMD alleged "data security failures caused injury to consumers whose sensitive personal information was disclosed without authorization in the 1718 File." *See* CCOB at 39 (capitalization omitted). In another statement of the issue, the FTC asserts that "[c]onsumers included in the 1718 File have been substantially injured by this

---

<sup>25</sup> If the FTC argument is to be accepted, then all of the evidence connected to Tiversa is "fruit" of such conduct which is questionable in best light. It should be eliminated from the FTC case, which in turn requires dismissal.

<sup>26</sup> The FTC focus on Richard Wallace as the singular "unauthorized" party who downloaded the 1718 File, to the exclusion of Tiversa as an entity or Boback as an individual actor, is contrary to the uncontroverted evidence in this case, and is erroneous.

disclosure of their sensitive, confidential, personal medical information.” *Id.* at 40 (footnote omitted).

(i) Unlawful conduct by Tiversa and FTC

By declaring Richard Wallace and Tiversa to be “unauthorized” third parties who downloaded the 1718 File, the FTC has further undercut its argument. All of the FTC evidence was the direct “fruit” of the 1718 File. *See* Sheer, Tr. at 31; *see also* Wallace, Tr. at 1344, 1353, 1362-70; RX0541 (Boback, Dep. at 36-42); CX0703 (Boback, Dep. at 142-143); RX0525 (Kaufman, Dep. at 20). *See generally* 42 U.S.C. § 1320d-6; Ga. Code Ann. § 16-9-93(a)-(c).

Consequently, CX 0307 (redacted), the 1718 File, and all derivative evidence – that is, the entire case – should have been excluded and the case dismissed. *Knoll Associates v. FTC*, 397 F.2d 530-37 (7th Cir. 1968).

The FTC may not use evidence or any of the fruits thereof that was/were wrongfully obtained. *See id.*; *see also Atlantic Richfield Co. v. Fed. Trade Comm’n*, 546 F.2d 646, 651 (5th Cir. 1977); *Fed. Trade Comm’n, v. Page*, 378 F. Supp. 1052, 1056 (N.D. Ga. 1974) (deterrence of governmental lawlessness served by application of the exclusionary rule regardless of the criminal or administrative nature of the proceedings).

Additionally, the FTC knew, or should have known, that neither Tiversa nor the Privacy Institute was authorized to obtain or disclose the individually identifiable health information contained on the 1718 File. It was unlawful for these entities, or the FTC, to do so. *See* 42 U.S.C. § 1320d-6. The FTC also knew, or should have known, that using the Privacy Institute as a PHI conduit made the government a party to conduct which violated HIPAA. *See* RX0644 (OGR Report, at 4, 54-62, 72-78, 89, 98-99).

(ii) Georgia tort law and privacy

Applying appropriate principles of Georgia tort law to the FTC arguments regarding privacy, the mere “disclosure is the harm” form of *per se* liability<sup>27</sup> is erroneous. The FTC is not empowered to pursue private causes of action under Section 5(n). Nor is the FTC empowered to prosecute HIPAA violations.

The FTC failed to prove *per se* liability because it did not adduce reliable, probative, and substantial preponderant evidence that the LabMD medical data security practices in 2007-2008 violated Section 5(n). The FTC characterization of the LabMD data security is irrelevant to the FTC burden of proof under Section 5(n), namely, that CC prove that the LabMD data security practices caused actual harm or are likely to cause substantial harm.

- (b) The FTC argument that a right to privacy in sensitive medical information satisfies Section 5(n)’s standards of proof by proxy is erroneous

In an admission of the deficiency of its proof regarding injury or likely substantial injury under Section 5(n), the FTC attempts to argue by analogy that the Tiversa theft of the LabMD file qualifies as an “unauthorized disclosure” under HIPAA, and therefore a private right of action lies against LabMD under Georgia tort law or HIPAA. That is, the “disclosure” to Tiversa proves both actual injury and likely substantial injury. *See* CCOB at 40-41. This argument has no basis in law or in fact.

The FTC citation to HIPAA and Georgia medical privacy statutes for the proposition that “Federal and state statutory law recognize individuals’ right to privacy in personal information, particularly medical information” is irrelevant. *Id.* at 40. The FTC reasons that somehow a “qualified right to privacy” under federal and Georgia law “demonstrates the broad recognition

---

<sup>27</sup> The CC new tort theory under Georgia law also sounds in quasi-strict liability. However, CC still must prove causation and injury.

of the inherent harm in the exposure of medical information. The exposure need not result in further injury – the mere disclosure is the harm.” *Id.* at 41.

The cases cited by the FTC do not support its theories of the “exposure” and “disclosure is the harm.” All cases sounding in tort under Georgia law require proof of causation and damages, as well as expert testimony as to the standard of care and injury. The case against LabMD is not analogous to these types of torts because the disclosure in this case was caused by intentional theft on the part of Tiversa, which in turn repeatedly violated state and federal law regarding PII and PHI by disclosing sensitive medical information to Professor Johnson and FTC.

Additionally, a theoretical cause of action for violation of privacy does not satisfy Section 5(n) which requires proof of actual injury or likely substantial injury causatively related to LabMD’s medical data security practices from June 2007 to May 2008.

Furthermore, an entirely theoretical cause of action based on Georgia tort law cannot lie because the harm complained of, exposure on Limewire in 2007-2008 and/or disclosure to Tiversa, is not the type of injury the statute was intended to guard against under the FTC theory of the case. *Cf. Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322 (11th Cir. 2012) (stolen laptops containing PHI and PII were “sold to an individual with a history of dealing in stolen property”); *see also Smith v. Triad of Alabama, LLC*, No. 1:14-cv-324-WKW-PWG, 2015 U.S. Dist. LEXIS 132514, at \*23-24 (M.D. Ala. Sept. 2, 2015) (Plaintiffs alleged “that they entrusted their PII/PHI to Defendant, that their PII/PHI was left unsecured, that a data breach occurred, that fraudulent tax returns were subsequently filed, and that they suffered economic damage/losses as a result.”).

FTC is not charged with enforcing HIPAA or Georgia tort law.

The FTC case was properly dismissed for failure to prove the first prong of Section 5(n)'s standard of proof.

**CONCLUSION**

For the reasons set forth herein, and any put forth forthwith at oral argument, this appeal should be dismissed, the Chief ALJ Chappell's Initial Decision affirmed, and judgment entered for Respondent.

Dated: February 5, 2016

Respectfully submitted,



Alfred J. Lechner, Jr.  
Daniel Z. Epstein  
Patrick J. Massari  
Cause of Action Institute  
1919 Pennsylvania Avenue, NW Suite 650  
Washington, DC 20006  
Phone: (202) 499-4232  
Facsimile: (202) 330-5842  
Email: [alfred.lechner@causeofaction.org](mailto:alfred.lechner@causeofaction.org)

*Counsel for Respondent, LabMD, Inc.*

**CERTIFICATE OF SERVICE**

**I hereby certify** that on February 5, 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

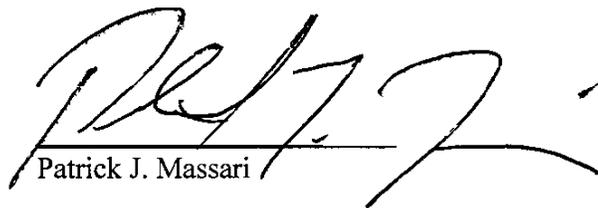
**I also certify** that I delivered via hand delivery and electronic mail copies of the foregoing document to:

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 Van Druff, 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

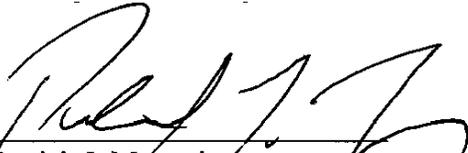
Dated: February 5, 2016

  
Patrick J. Massari

**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: February 5, 2016



Patrick J. Massari

Notice of Electronic Service

**I hereby certify that on February 05, 2016, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s Corrected Answering Brief, 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 February 05, 2016, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s Corrected Answering Brief, 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  
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

Alfred Lechner  
President & CEO  
Cause of Action Institute  
jlechner@causeofaction.org  
Respondent

Patrick Massari  
Attorney