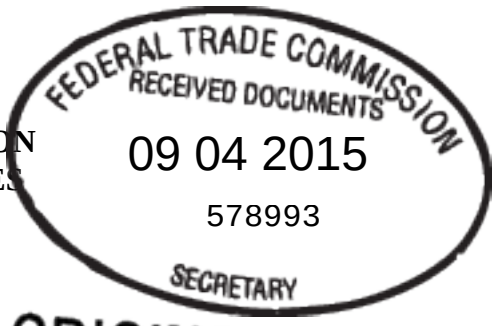
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES



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

ORIGINAL

COMPLAINT COUNSEL'S REPLY TO
RESPONDENT'S POST-TRIAL BRIEF

Alain Sheer
Laura Riposo VanDruff
Jarad Brown
Ryan Mehm
Megan Cox

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

Complaint Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Constitutional Provisions

Statutes

Regulations

Cases

Administrative Materials

Other Authorities

REFERENCE ABBREVIATIONS

References to the parties' proposed findings, conclusions, and replies to proposed findings and conclusions are made using the following abbreviations:

CCFF – Complaint Counsel's Proposed Findings of Fact

CCCL – Complaint Counsel's Proposed Conclusions of Law

CCRRFF – Complaint Counsel's Reply to Respondent's Proposed Findings of Fact

CCRRCL – Complaint Counsel's Reply to Respondent's Proposed Conclusions of Law

RFF – Respondent's Proposed Findings of Fact

RCL – Respondent's Proposed Conclusions of Law

INTRODUCTION

Respondent ignores the core of this case, and the reasons the Commission pursued it: LabMD's business model depended upon gathering the most sensitive types of Personal Information about hundreds of thousands of consumers in connection with providing laboratory test results. This sensitive personal information included Social Security numbers, names, addresses, dates of birth, and medical information including information about health insurance and health testing codes, all of which Respondent had a duty to protect. Nevertheless, over a multi-year period Respondent failed to provide reasonable security to protect the Personal Information of 750,000 consumers, most of whom were unaware that LabMD would receive and keep their most sensitive Personal Information. The evidence in this case conclusively demonstrates that Respondent:

- Failed to have a comprehensive written information security program;
- Failed to use reasonable, readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities;
- Failed to use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- Failed to adequately train employees to safeguard personal information;
- Failed to require employees to use common authentication-related security measures;
- Failed to maintain and update operating systems and other devices; and
- Failed to employ readily available measures to prevent or detect unauthorized access to personal information.

LabMD's unreasonable data security practices caused or are likely to cause substantial injury to consumers in violation of the FTC Act's prohibition of "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). These harms include, but are not limited to, identity theft, medical identity theft, tax identity theft, loss of privacy in sensitive medical information, and loss of time spent dealing with the consequences of those failures. Consumers generally had no choice of laboratory to obtain test results, and could not reasonably avoid these harms. LabMD could have corrected many of its failures at low cost; its failure to do so provided no countervailing benefits to consumers or competition.[1] Given these circumstances, entry of the Notice Order is appropriate.

None of the arguments in Respondent's post-trial brief justify or excuse its violation of Section 5 of the FTC Act. The Commission already rejected Respondent's central argument that HIPAA preempts the FTC Act, and Respondent conceded in a verified discovery response that HIPAA is irrelevant to this proceeding. Even if HIPAA were relevant (it is not), Respondent has never shown it was in full compliance.

Respondent's attempts to distract the Court with irrelevant details regarding a third-party witness do nothing to obscure the overwhelming evidence Complaint Counsel has introduced in this case demonstrating LabMD's systemic and utter failure to employ reasonable data security practices.

---

[1] These unfairness elements, codified in Section 5(n) of the FTC Act, set forth Complaint Counsel's burden of proof, contrary to Respondent's assertion that "this case raises multiple issues of first impression, including Complaint Counsel's burden of proof under Section 5(n)." Complaint Counsel's burden of proof is an issue that has been resolved since at least 1994 when Section 5(n) was adopted. Pub.L. 103-312 § 9 (Aug. 26, 1994).

While Respondent further attempts to distract the Court with alleged violations of the Appointments Clause, due process, and the Administrative Procedure Act, these arguments are without merit and contrary to settled law. This proceeding does not violate any Constitutional or statutory provisions.

Contrary to Respondent's assertions, Complaint Counsel has proven its case under Section 5 of the FTC Act. Respondent has failed to rebut the mountain of evidence that its multiple and serious failures to protect personal information are likely to cause substantial injury to consumers, and that these harms are not outweighed by any countervailing benefits to consumers or to competition.

Respondent's inadequate security practices are likely to continue harming consumers absent a court order. Complaint Counsel has therefore submitted a Notice Order that will require Respondent to, among other things, adopt a comprehensive information security program, obtain biennial security assessments, and notify consumers Respondent impacted by its data security failures. Respondent has offered no legal authorities precluding entry of the Notice Order in these proceedings. For these reasons and as set forth in Complaint Counsel's post-trial briefing, entry of the Notice Order is appropriate to address Respondent's security failures and protect consumers.

FACTS

I. Background

A. LabMD

LabMD created a computer network to collect, several times a day in some cases, CCFF ¶ 86, the most sensitive Personal Information of consumers—even consumers to whom it provided no services. CCFF ¶¶ 79, 84-85, 89. LabMD failed to provide reasonable security for

that data, in violation of Section 5's prohibition of unfair acts or practices. Its failure caused or is likely to cause substantial harm to consumers that they could not reasonably avoid, and that harm is not offset by any countervailing benefits to consumers or competition.

Importantly, countervailing benefits are determined based on the specific practice at issue in a complaint, not the overall operation of a business.[2] *FTC v. Accusearch, Inc.*, 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007), judgment aff'd *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009) ("While there may be countervailing benefits to some of the information and services provided by 'data brokers' such as *Abika.com*, there are no countervailing benefits to consumers or competition derived from the specific practice of illicitly obtaining and selling confidential consumer phone records." (emphasis original)); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (upholding Commission finding of no countervailing benefits because an increase in fees "was not accompanied" by an increased level or quality of service); *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 2 (Jan. 15, 2014) (reiterating that countervailing benefit determination is made by "compar[ing] that harm to any benefits from that particular practice"). Countervailing benefits are unlikely to be significant when more effective security measures could have been implemented at relatively low cost, which LabMD could have done. *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290, at *97

---

[2] Complaint Counsel does not dispute, for the most part, LabMD's description of the operation of its business. For a complete discussion, see CCRRFF ¶¶ 12-34. To the extent Respondent claims that LabMD operated more quickly, efficiently, or accurately than its competitors, the testimony to which it cites does not describe LabMD's process in relation to pre-existing or competing processes, but merely contains conclusory statements that it is so. This evidence fails to prove any countervailing benefits, which, as described in the text, is irrelevant—the question at hand is not the benefit of LabMD's processes, but the benefit of its unreasonable data security. *See infra* Argument, § II.C.3 (Complaint Counsel has Proven that LabMD's Unfair Practices Caused or Likely Caused Substantial Injury to Consumers), at 128-31.

(1984) (Unfairness Statement) (stating that "[m]ost business practices entail a mixture of economic and other costs and benefits for purchasers" and framing the evaluation as to whether a practice is "injurious in its net effects," taking into account the "various costs that a remedy would entail"); CCFF ¶¶ 1113-1185 (describing various low- and no-cost measures LabMD could have taken to correct its unreasonable security failings).

1. LabMD Did Not Seek Expert Advice on Data Security[3]

LabMD claims that it hired companies and individuals with extensive experience in medical laboratory industry IT design, systems implementation, and operations to design, manage and maintain the company's IT network, laboratory processes and data security; and that it sought and relied on expert advice and ran a compliant system. Resp't's Post-Trial Brief at 6. However, this claim is contradicted by the record. LabMD cites the testimony of Mr. Boyle, LabMD's Vice President for Operations and General Manager from November 2006 to August 2013, and Mr. Truett, the owner of APT, a company that provided computer and network service to LabMD through approximately March 2007, CCFF ¶ 182, to support its claim. The evidence, as detailed below, however, demonstrates that LabMD did not rely on the employees or outside experts Respondent identified to manage and maintain its IT network and data security.

Mr. Boyle entered the medical testing field as a laboratory technician, and his education is in microbiology, chemistry, and Latin. CX0704-A (Boyle, Dep. at 91-96). Prior to joining LabMD, Mr. Boyle never had primary responsibility for data security, and did not recall what tools those who had primary responsibility used. CX 0704-A (Boyle, Dep. at 115, 117-118). The main IT responsibility in his prior employment about which he testified was selecting new

[3] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

laboratory and billing programs, and there is no evidence that he took data security into consideration in making that decision. CX 0704-A (Boyle, Dep. at 108-109).

APT did not manage or maintain LabMD's IT network or data security. APT monitored LabMD's network only in response to problems raised by LabMD employees, such as Internet speed and connectivity. CX0731 (Truett, Dep. at 69, 78-79). APT did not evaluate the criticality of potential risks to LabMD's system, as this was not a service APT ever provided to any of its clients. CX0731 (Truett, Dep. at 118-119). APT did not provide data security services in connection with any administration of servers and firewalls it provided to LabMD. Mr. Truett testified that APT's work concerning the administration of servers and firewall systems would be limited to "maybe a user management function, a user forgot their password." CX0731 (Truett, Dep. at 31-32). APT did not examine network traffic in and out of LabMD. Mr. Truett testified that "[w]e didn't do any monitoring or log reviews unless it was ad hoc," that any such ad hoc reviews conducted were to resolve a non-security issue such as "Internet speeds, connectivity problems," and that APT did not provide log review as a service. CX0731 (Truett, Dep. at 69). APT did not patch LabMD's system. Mr. Truett could not recall how service packs and software patches were applied at LabMD, but stated that APT's general practice was to verify that patches and updates were loaded at client sites only when called to handle a breakdown or fix issues that had come up. CX0731 (Truett, Dep. at 32). Furthermore, APT ceased providing services to LabMD in or around March 2007. CCRRFF ¶ 136 (APT ceased providing services to LabMD around March 2007). In late 2006 and 2007, LabMD replaced APT's services with additional internal IT employees that it hired. CX0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions) at 5; CX0733 (Boyle, IHT at 64-65); CX0731 (Truett, Dep. at 28-29).

Finally, while LabMD claims it relied on its employees to maintain its data security, it claims *in this proceeding* that Curt Kaloustian – whose responsibilities from October 2006 to April or May 2009 included maintaining servers, patches, and upgrades, CCFF ¶¶ 349-350 – was "not qualified in any way to meet the demands of his position with LabMD," RFF ¶ 239, and was terminated for "inadequate work performance." RFF ¶ 376. Mr. Kaloustian had primary responsibility for, among other things, LabMD's network security, firewall security, servers, determining how to protect desktop computers, and setting up antivirus and administrative profiles on employee laptops. CX0730 (Simmons, Dep. at 16, 125-26 (Kaloustian managed firewall), 156 (Kaloustian would have been responsible for monitoring outbound traffic on LabMD's network); CX0734 (Simmons, IHT at 21 (Kaloustian was in charge of security firewall), 35 and 169-170 (maintaining servers was Kaloustian's responsibility), 54-55 and 164 (backups were Kaloustian's domain), 57 (Kaloustian was in charge of hardware, servers, and networks), 75 (Kaloustian and Simmons determined how to protect desktop computers), 86-87 (Kaloustian was in charge of network security), 103 (Kaloustian cleaned up infected computers at physician-clients' offices), 104-05 (Kaloustian managed software firewalls), 115-116 and 119-120 (Kaloustian installed antivirus on sales employees' laptops), 161 (Kaloustian was employee who would have monitored Internet traffic); *see also* CX 0704-A (Boyle, Dep. at 10 (Mr. Kaloustian was at LabMD when Mr. Boyle started), 147 (describing how Kaloustian worked on a hardware issue with the Lytec server); CX0736 (Daugherty, IHT at 49). If Mr. Kaloustian was unqualified, LabMD nonetheless gave him astonishing responsibility.

2. LabMD's Employee Handbook Was Not a Comprehensive Written Information Security Program

LabMD also claims that its Employee Handbooks emphasized repeatedly that employees had a mandatory duty to protect PHI and that failure to do so would result in termination.

Although the Handbook may have told employees not to share customer information, it did not tell employees that they needed to take steps to *secure* PHI or any other information from unauthorized access, or how to secure it from such access. Its only specific policy even arguably relating to information security is a restriction on personal Internet and email usage. CX0001 (LabMD Employee Handbook Rev. June 2004) at 7; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 7. LabMD's Employee Handbook does not include policies for encrypting sensitive information in or attached to emails. CX0001 (LabMD Employee Handbook Rev. June 2004); CX0002 (LabMD Employee Handbook Rev. Mar. 2008). LabMD's Employee Handbook does not include password policies. CX0710-A (Daugherty, LabMD Designee, Dep. at 119); CX0001 (LabMD Employee Handbook Rev. June 2004); CX0002 (LabMD Employee Handbook Rev. Mar. 2008).

Under a section entitled "Privacy of Protected Information," LabMD's Employee Handbook states that "LabMD has taken specific measures to ensure [its] compliance with" HIPAA. CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6. The handbook does not describe any of the "specific measures" taken to ensure compliance with HIPAA. CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6. No "specific measures" that LabMD took to comply with HIPAA were identified to LabMD employees. CX0714-A ([Fmr. LabMD Empl.], Dep. at 88-89); CX0716 (Harris, Dep. at 51); CX0707 (Bureau, Dep. at 26). And no LabMD employee — including LabMD's President and CEO — could describe what mechanisms LabMD implemented to achieve the stated goal of "specific measures" to comply with HIPAA. CX0725-A (Martin, Dep. at 166-67); CX0711 (Dooley, Dep. at 144-46); CX0719 (Hyer, Dep. at 162-63); CX0733 (Boyle, IHT at 248-49);

CX0710-A (Daugherty, LabMD Designee, Dep. at 131-132; 135-137). Ultimately, no matter how LabMD attempts to characterize it, the 22-page Handbook, which addresses such diverse issues as harassment, tardiness, equal employment, uniforms, and workplace safety, does not remotely qualify as a comprehensive written information security program.

B. Precomplaint Investigation[4]

1. Third Party Witness Tiversa

Complaint Counsel's precomplaint investigation is irrelevant to the disposition of this proceeding. As this Court noted, "[o]nce the Commission has . . . issued a complaint, the issue to be litigated is not the adequacy of the Commission's pre-complaint information or the diligence of its study of the materials in question but whether the alleged violation has in fact occurred." Order Granting in Part and Denying in Part Compl. Counsel's Mot. to Quash Subpoena on Compl. Counsel and for Prot. Order, at 5-6 (Jan. 30, 2014) (citing *Exxon Corp.*, 83 F.T.C. 1759, 1974 FTC LEXIS 226, at *2-3 (1974)); *see also* Order Denying Resp't's Mot. for a Rule 3.36 Subpoena, at 4-5 (Feb. 21, 2014); Order Granting Compl. Counsel's Mot. to Quash and to Limit Dep. Subpoenas Served on Comm'n Att'ys, at 2-7 (Feb. 25, 2014); Order Granting in Part and Denying in Part Compl. Counsel's Mot. for Prot. Order Regarding Rule 3.33 Notice of Dep., at 4 (March 10, 2014). The Commission initiates investigations based on a variety of sources. *Cf. Osborne v. Grussing*, 477 F.3d 1002, 1007 (8th Cir. 2007) (agencies routinely act on the basis of information provided by private parties with a personal interest, and "[w]hen such a complaint results in enforcement action, we do not impute the complainant's ulterior motive to

[4] Complaint Counsel's subheading structure differs from Respondent's in this section. Complaint Counsel's Section I.B.1 responds to Respondent's Sections I.B.1-I.B.3. *See* Resp't's Post-Trial Brief at 7-23. Complaint Counsel's Section I.B.2 responds to Respondent's

the government enforcers"). Complaint Counsel performed a thorough investigation of the full spectrum of LabMD's data security practices. *See* evidence discussed at CCFF ¶¶ 382-1110.

There is no dispute that the 1718 File was available on a P2P network. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 4, Stip. 11). The factual record is likewise uncontroverted that Tiversa downloaded the 1718 File in February 2008. Wallace, Tr. 1393-95. Three months later, LabMD was advised that the 1718 File was available through LimeWire. CCFF ¶ 1395. More than a year elapsed before the 1718 File was provided to the Commission in response to a Civil Investigative Demand. *See* Wallace, Tr. 1352-1353,1361-1362, 1365, 1385-1386.

Respondent attempts to distract from these undisputed facts. First, Respondent uses innuendo and hyperbole to suggest that Complaint Counsel engaged in misconduct. These allegations are unfounded and untrue, and they are unsupported by any evidence in the record. Second, Respondent suggests that Tiversa Holding Corporation's[5] business practices, research partnerships, and role in Complaint Counsel's precomplaint investigation somehow taint this entire proceeding or violate Respondent's due process rights. Its position in this regard is incorrect as a matter of fact[6] and as a matter of law. *See infra* Argument, § I.C.2 (LabMD's Due

---

characterization of Commission staff's testimony at a July 24, 2007, hearing before the House Oversight Committee. *See* Resp't's Post-Trial Brief at 10-11.

[5] The parties obtained discovery from Tiversa Holding Corporation, not Tiversa, Inc. Complaint Counsel nonetheless responds herein as if Respondent had defined "Tiversa" to mean Tiversa Holding Corporation. To the extent that Respondent's post-trial briefing relates to Tiversa, Inc., the Court should disregard the proposed findings of fact, conclusions of law, and briefing because they are not supported by the evidentiary record.

[6] Respondent's characterization of the staff report prepared for Representative Issa (RX644 (not admitted for the truth of the matters asserted therein)), Resp't's Post-Trial Brief at 23, violates the Court's July 15, 2015 Order, which imposed significant "limitations and qualifications as to [the] evidentiary use" of RX644. Order on Resp't's Mot. to Admit Exhibits at 3 (July 15, 2015).

Process Rights Under the Fourth Amendment Have Not Been Violated in This Proceeding), at 69-74.

Tiversa is a third-party witness. Through its Rule 3.33 designee, Robert Boback, Tiversa was deposed by the parties on November 21, 2013. CX0703 (Boback, Tiversa Designee, Dep.). Respondent's counsel conducted a thorough examination. CX0703 (Boback, Tiversa Designee, Dep. at 97-164). It is the Court's role to make determinations of credibility regarding Mr. Boback's testimony. However, such determinations are unnecessary here because Complaint Counsel's post-trial brief and proposed findings of fact do not cite to or rely on Mr. Boback's testimony, CX0019, or expert conclusions that were predicated on Mr. Boback's testimony. *See* Compl. Counsel's Post-Trial Brief at 61 n.3 (August 10, 2014).[7]

2. The Commission Provided Business Guidance[8]

Respondent implies that the Commission testified there was no risk associated with P2P technology by selectively quoting FTC staff's testimony before the House Oversight Committee in 2007. Commission staff in fact testified that P2P technology presented considerable risk to businesses and consumers. While the Commission's written testimony recited that a 2005 staff report had described P2P software as a "neutral technology," meaning that the technology itself

---

The Court should disregard all such characterizations. *See infra* Facts, § I.C (Respondent's Citation to Facts in RX655 Violates the Court's Order), at 16.

[7] In some instances below, Complaint Counsel cites to Mr. Boback's testimony for the narrow purpose of responding to Respondent's factual and legal assertions. As noted, in these instances, it is the Court's role to make determinations of credibility regarding Mr. Boback's testimony.

[8] Complaint Counsel's Section I.B.2 responds to Respondent's characterization of Commission staff's testimony at a July 24, 2007 hearing before the House Oversight Committee. *See* Resp't's Post-Trial Brief at 10-11; *see also* n.6, above.

could be used safely, it noted that user behavior could create risk. CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 2-3. The Commission's statement also explained that P2P technology created the risk that users "may unintentionally share personal or other sensitive files residing on their hard drives." *Id.* at 3. The statement also set forth the steps that the Commission had taken to warn consumers and businesses of the dangers of P2P file sharing as early as July 2003. *Id.* at 9-12. At most, the statement indicated that there might be possible legitimate uses for P2P sharing technology for businesses. *Id.* at 4. LabMD had no business need for LimeWire. *See* CCFF ¶ 1371; *see generally* CCFF ¶¶ 1363-1390.

Respondent also argues that it complied with the guidance contained in the Commission's business publication, *Protecting Personal Information: A Guide For Business* ("Protecting Personal Information"). Resp't's Post-Trial Brief at 19 n.4. First, Respondent argues that the Commission did not provide this guidance until 2011. This is factually incorrect. The Commission first released *Protecting Personal Information*, containing the five basic steps to create an information security program discussed below, in March 2007. *See* Press Release, FTC, FTC Unveils Practical Suggestions for Businesses on Safeguarding Personal Information (Mar. 8, 2007), *available at* https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding. It has updated the guide multiple times since then, as information security has evolved.

Second, as to the substance, the five basic steps described in the Commission's 24-page *Protecting Personal Information* business guide are: (1) Take Stock: Know what personal information you have in your files and on your computers. (2) Scale Down: Keep only what you need for your business. (3) Lock it: Protect the information that you keep (covering both physical and electronic security) (4) Pitch it: Properly dispose of what you no longer need. (5)

Plan Ahead: Create a plan to respond to security incidents. FTC, *Protecting Personal Information: A Guide for Business* at 3, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. In this regard, the FTC's business guidance embraces the concept of having multiple layers of protection for data. These considerations are consistent with the network security principles identified by Dr. Hill. Indeed, implementing reasonable security requires consideration of, and of course reliable implementation of, fundamental data security principles, no matter how they are articulated.[9]

Both Dr. Hill's report and *Protecting Personal Information* address these fundamental data security principles. Dr. Hill's "Don't Keep What You Don't Need," CX0740 ¶ 31(a), is the same concept as "Scale down. Keep only what you need for your business." *Protecting Personal Information* at 2, 6-9. Dr. Hill's "Patch" admonition, CX0740 ¶ 31(b), is the same as the guide's recommendation to "check expert websites (such as www.sans.org) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems." *Protecting Personal Information* at 10. Dr. Hill's discussion of "Ports," CX0740 ¶ 31(c), is consistent with the recommendation to "consider closing the ports to those services on that computer to prevent unauthorized access to that machine." *Protecting Personal Information* at 10. Dr. Hill's section on "Policies" relates to

[9] The principles addressed herein are consistent with the requirements of the Security Rule promulgated by the Department of Health and Human Services. *See* 45 C.F.R. Pts. 160, 164 (subparts A and C). *See* Comm'n Order Denying Resp't's Mot. to Dismiss, at 11 (Jan. 16, 2014) ("[T]he patient-information protection requirements of HIPAA are largely consistent with the data security duties that the Commission has enforced pursuant to the FTC Act"); *id.* at 12 ("HIPAA evinces no congressional intent to preserve anyone ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act").

data access, passwords, and backups, CX0740 ¶ 31(d), topics covered in the "Password Management" section of the guide and its recommendation to "consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices." *Protecting Personal Information* at 10, 12-13. Dr. Hill's "Protect" recommendation regarding the use of security software like firewalls, anti-spyware, anti-virus, and intrusion detection software, along with authentication and access controls, CX0740 ¶ 31(e), is consistent with the guide's recommendation to implement firewalls (at 14), regularly run up-to-date anti-virus and anti-spyware programs (at 10), consider use of an intrusion detection system (at 16), and have strong password policies (at 12-13). Finally, Dr. Hill's discussion concerning "Probe," recommending a security audit that tests the state of the network, CX0740 ¶ 31(f), is consistent with the guide's recommendation to "[a]ssess the vulnerability of each connection to commonly known or reasonably foreseeable attacks," which "may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit." *Protecting Personal Information* at 10.

Furthermore, Respondent misrepresents LabMD's implementation of the guidelines in *Protecting Personal Information*. LabMD kept far more information than it needed, including the Personal Information of more than 100,000 consumers for whom it never performed testing. CCFF ¶ 79; *see also Protecting Personal Information* at 6-7 ("Scale Down"). LabMD failed to regularly purge the Personal Information of the consumers for whom it never performed testing through its database application, although it could have done so at relatively low cost. CCFF ¶¶ 1152-1154. The purging of such unneeded data was a regular practice of IT practitioners throughout the Relevant Time Period. CCFF ¶ 1154. LabMD did not have a secure network. Its firewalls did not operate in some instances and were not properly configured when they did

operate, and LabMD did not record or review the firewall logs to determine if unauthorized traffic was crossing its network. CCFF ¶¶ 631-657, 1075-1105; *see also Protecting Personal Information* at 9. Its antivirus software was at times inadequate, out-of-date, not centrally managed, and antivirus scans were not consistently run and reviewed. CCFF ¶¶ 527-629; *see also Protecting Personal Information* at 10. While LabMD may have shredded incomplete day sheets and aging reports, as recommended by the guide's "Pitch it" principle, Resp't's Post-Trial Brief at 19 n.4; *but see* (CX0714-A ([Fmr. LabMD. Empl., Dep. at 53-54) (Former LabMD Employee did not shred papers containing sensitive Personal Information when she was done with them, but placed them in the recycle bin), it has stored indefinitely all the *complete* Day Sheets it has created since it has been in business, in addition to scanning some of them electronically. CCFF ¶¶ 157-161; *see also Protecting Personal Information* at 20-21. It also retained copies of consumers' credit card numbers and personal checks for years. CCFF ¶¶ 136-148. In fact, LabMD has never destroyed any of its copies of consumers' checks, and has all the copies of checks it has made since the company's inception, and it scanned and stored some of its copies electronically. CCFF ¶¶ 147-148. All this data is in addition to the electronic Personal Information of 750,000 consumers. CCFF ¶ 78. LabMD did not provide reasonable security for the Personal Information it maintains under any analysis.

C. Respondent's Citation to Facts in RX644 Violates the Court's Order

Respondent's discussion of a congressional staff investigation of and citations to facts asserted in a staff report violate this Court's July 15, 2015 Order. Respondent's assertion that "[t]he staff investigation makes many notable claims, and purports to provide independent email and telephone record evidence to support same," Resp't's Post-Trial Brief at 23, violates the Court's order to the extent the findings of the report are cited to demonstrate the truth of the

matters therein. Order on Resp't's Mot. to Admit Exhibits at 3 (July 15, 2015). To the extent the statement is meant to show only that the report reached these conclusions but not to show that they are true, then the statement is irrelevant and useless to any claim or defense in this proceeding. The content of the congressional staff report, therefore, has no bearing on this case.

II. LabMD Did Not Adopt or Implement Reasonable Data Security Policies, Practices and Procedures

A. The Evidence Establishes that LabMD Did Not Adopt or Implement Reasonable Data Security Policies, Practices and Procedures

1. LabMD's Handbook Did Not Establish Reasonable Data Security Policies, Practices, and Procedures, and LabMD Did Not Reasonably Implement Its Policies[10]

Reasonable security is not accomplished merely by publishing a statement about compliance with existing laws in an employee handbook and then claiming that all employees acknowledged receiving and understanding the handbook. CCRRFF ¶ 92. LabMD failed to train its employees in using appropriate measures to protect Personal Information. CCFF ¶¶ 852-900. Measures are needed to assure compliance because employees make mistakes and are often unaware of the consequences of non-compliance. CCFF ¶ 853-854. Adequate security policies are therefore more than mere prohibitions: they should be in writing, identify goals and mechanisms to achieve the goals, including enforcement mechanisms and training so employees understand how to comply. CCFF ¶¶ 388, 411, 853-854. And reasonable security requires a comprehensive set of policies that address a variety of reasonably foreseeable security issues and concerns. CCFF ¶¶ 397-401.

[10] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

LabMD's handbook itself makes clear that mere prohibitions are not enough for reasonable security. Its Statement of Purpose and Ethics Policy purports to set out a plan for implementation, which include "keeping employees . . . educated, informed, and trained," making "compliance everyone's job," and requiring LabMD to establish "a formal structure to monitor, detect, respond to, and correct violations of applicable federal, state and local laws, and regulations, as well as violations of Standards of conduct and LabMD policies," and providing "mechanisms and resources broad enough to accomplish this objective." CX0001 (LabMD Employee Handbook rev. June 2004) at 3.

LabMD systematically failed to meet its own standard. Its handbook asserts that HIPAA prohibits unauthorized disclosures of protected health information. The handbook further claims that LabMD took "specific measures to ensure our compliance" with HIPAA. CX0001 (LabMD Employee Handbook rev. June 2004) at 6. However, no LabMD employee, including Mr. Daugherty, was able to identify a single security measure taken to ensure HIPAA compliance. CCFF ¶¶ 427-431. LabMD also argues that its employees testified that LabMD had "measures in place designed to protect PHI including written policies" on a number of security topics. Resp't's Post-Trial Brief at 24. As discussed in Facts, Section II.A.2 (LabMD's Former Employees' Testimony Establishes that LabMD Did Not Adopt or Implement Reasonable Data Security Policies, Practices and Procedures), at 18-27, below, LabMD's employees did not testify consistently to any such thing. Even where LabMD did have policies in place, they were ineffectual or not coupled with any enforcement mechanism. CCFF ¶¶ 446-455 (§ 4.2.3 When LabMD Finally Prepared Written Information Security Policies in 2010, They Were Incomplete), ¶¶ 458-480 (§ 4.2.4 LabMD Did Not Enforce Some of the Policies in Its Policy Manuals).

2. LabMD's Former Employees' Testimony Establishes that LabMD Did Not Adopt or Implement Reasonable Data Security Policies, Practices and Procedures

a. Ms. Harris, [Former LabMD Employee], Ms. Brown, and Ms. Gilbreth Did Not Testify to Reasonable Data Security Policies, Practices, and Procedures

Respondent cites to a selected portion of its former employees' testimony to support its claim that LabMD had measures in place to protect Personal Information. Resp't's Post-Trial Brief at 24-28. However, Respondent's citations do not support even the limited practices it claims were in place.

LabMD claims that Ms. Harris, [Former LabMD Employee], and Ms. Gilbreth testified to receiving yearly training in areas such as LabMD compliance standards, HIPAA, limited use of computer systems, internet restrictions, playing CDs, and downloads from the Internet. However, Ms. Harris testified that she did not receive any training on HIPAA (privacy and security) or the other items in LabMD's compliance program: the False Claims Act, Anti-Kickbacks, and Stark II. CX0716 (Harris, Dep. at 62-63). Ms. Harris testified that she received training only on limited Internet access, playing CDs, and downloading items from the Internet. CX0716 (Harris, Dep. at 62-63). [Former LabMD Employee] testified that she watched a non-LabMD specific video on HIPAA upon joining the company, and testified that the only other training she received at LabMD had to do with her job duties, not with privacy or security. CX0714-A ([Fmr. LabMD Empl.], Dep.at 86-87). Ms. Gilbreth did not provide any details on the training she testified to receiving. CX0715-A (Gilbreth, Dep. at 77). However, she testified that when she provided training to new billing employees, she highlighted particular areas, "primarily having to do with how the vacation time is laid out, and that using personal e-mail

was unacceptable."[11] CX0715-A (Gilbreth, Dep. at 83). She did not know any specific measures LabMD took to comply with HIPAA, and did not identify any such specific measures to new employees. CX0715-A (Gilbreth, Dep. at 83-84). This testimony is consistent with the Complaint Counsel's evidence proving that LabMD did not adequately train its employees to safeguard Personal Information. CCFF ¶¶ 852-900.

LabMD claims that its employees testified that LabMD limited their Internet access to insurance companies' websites. However, both Ms. Harris and Ms. Brown testified that they never attempted to access websites other than those of insurance companies, and did not know if technical restrictions would actually have prevented them from doing so. CX0716 (Harris, Dep. at 82-83); CX0706 (Brown, Dep. at 115-16). Ms. Gilbreth testified that she did not recall such restrictions being in place before 2010. CX0715-A (Gilbreth, Dep. at 64). Prior to the restrictions going into place, possibly in 2010, Ms. Gilbreth testified that there were no restrictions on her access to the Internet, and no technical computer restrictions prevented her from downloading any application that she wanted from the Internet. CX0715-A (Gilbreth, Dep. at 64-65). This testimony is consistent with the fact that LimeWire was downloaded and

---

[11] LabMD claims that Ms. Gilbreth provided training to new employees based on the employee handbook and an unspecified "security handbook." Resp't's Post-Trial Brief at 27-28. This characterization is not supported by the evidentiary record. Ms. Gilbreth's testimony never identified any "security handbook." CX0715-A (Gilbreth, Dep. at 81-86) (identifying only CX0002, LabMD's Employee Handbook, as a document she recognized in full). She stated that she had some familiarity with CX0006, LabMD's policy manual, but recognized only some of the paragraphs through the first couple of pages. CX0715-A (Gilbreth, Dep. at 84-85). She did not testify to providing training based on CX0006, and testified that only "parts of it are familiar" to her. CX0715-A (Gilbreth, Dep. at 85-86)). Likewise, LabMD claim that Ms. Gilbreth was "familiar with portions of the LabMD policy manual and the 'IT Security Handbook.'" Resp't's Post-Trial Brief at 27-28. The cited testimony refers only to one document, CX0006, and Ms. Gilbreth, as noted above, testified only that "parts of it are familiar to her," did not specify which parts, and did not discuss any data security steps taken in response to the document. CX0715-A (Gilbreth, Dep. at 85-86).

installed onto a LabMD computer in or about 2005, and remained on that computer undetected until 2008, when LabMD was informed that it was sharing the 1718 File on a P2P network. CCFF ¶¶ 1363-1365.

LabMD claims that its employees testified that it was company practice to shred paper copies of insurance aging reports when no longer needed. First, this does not address LabMD's practice of storing electronic copies of files with highly sensitive Personal Information, including insurance aging reports, on an employee's workstation. CCFF ¶ 1072. LabMD's Policy Manuals[12] both dictate that a copy of the backup file from LabMD's Lytec billing software should be daily saved to the Finance Manager desktop PC; these backups contained all of the patient, client, and billing information related to work performed through LabMD. CCFF ¶¶ 1070-1071. Information stored on an employee's workstation, as required by the Policy Manuals, is vulnerable because an employee may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, and other threats. CCFF ¶ 1068.

Second, the testimony Respondent cites does not support its claim that unneeded insurance aging reports were shredded. While Ms. Gilbreth stated that aging reports were shredded, CX0715-A (Gilbreth, Dep. at 14-16), [Former LabMD Employee] testified that she placed aging reports in the recycle bin, and did not shred them. CX0714-A ([Fmr. LabMD. Empl.], Dep. at 55). [Former LabMD Employee] did not use any shredders, nor did she know of any employee who used shredders. CX0714-A ([Fmr. LabMD. Empl.], Dep. at 55). Ms. Harris

[12] Although LabMD created in 2010 written Policy Manuals addressing limited aspects data security, the Policy Manuals failed to address key security policies, and LabMD did not enforce some of the policies in them. CCFF ¶¶ 446-480.

testified that while she shredded aging reports, she could not "account for what everyone else" in the billing department did with paper copies of insurance aging reports. CX0716 (Harris, Dep. at 40-41). Finally, while Ms. Brown testified that she shredded insurance aging reports, she worked on-site at LabMD only from May 2005 through May 2006; from May 2006 until leaving LabMD in March 2013, Ms. Brown worked from home and went to the office once per month. CX0706 (Brown, Dep. at 6-7, 143-44). She was not in a position to observe the regular practice of other LabMD employees. This contradictory testimony indicates there was no set policy that all employees were following, consistent with the evidence Complaint Counsel has presented showing LabMD's lack of security policies in general and its failure to implement the limited, inadequate policies that it had. CCFF ¶¶ 397-480.

LabMD also claims its employees testified it "had in place" different sets of login credentials for computers and for the Lytec billing system. Resp't's Post-Trial Brief at 25-26. But its claim is not supported by the testimony. On the contrary, no employee could confirm that there were any written or technically-enforced requirements for credentials to be different for employees' computers and other systems into which they logged in. Ms. Harris and [Former LabMD Employee] testified that they had different credentials, but did not testify to whether there was any requirement for them to do so. CX0716 (Harris, Dep. at 69); CX 0714-A ([Former LabMD Employee], Dep. at 43-45). Furthermore, the evidence shows that LabMD did not have policies or procedures in place to ensure employees used unique passwords. (CCFF ¶¶ 919-951).

b. **Mr. Dooley Did Not Testify to Reasonable Data Security Policies, Practices, and Procedures**

Respondent's reliance on Jeremy Dooley's deposition testimony to establish the status of LabMD's firewalls is misplaced. Mr. Dooley testified that he is not a security expert. CX0711 (Dooley, Dep. at 31). While he did testify generally that LabMD had firewalls, he did not

describe how they were set up or state that they were done so correctly. CX0711 (Dooley, Dep. at 31). In fact, he expressly stated that he was not sure that he was "qualified to answer" questions about security. CX0711 (Dooley, Dep. at 31). Nor can Mr. Dooley's testimony establish that "[b]oth the lab software and the billing software had separate firewall routers." Resp't's Post-Trial Brief at 28. Mr. Dooley testified that a firewall router is "a device that has – as incoming Internet traffic is received, it routes that." CX0711 (Dooley, Dep. at 24, 72). Mr. Dooley does not describe any firewall functions, such as blocking unwanted traffic or blocking traffic to unauthorized applications. *See, e.g.*, CCFF ¶¶ 1075-1081 (describing the functions of firewalls). Furthermore, the evidence shows that LabMD's router was not configured to provide firewall protection at its Powers Ferry Road location. CCFF ¶ 1086. LabMD's routers also did not have logging capability, CCFF ¶ 246, were not tested for vulnerabilities, CCFF ¶¶ 178-179, and LabMD had no written policy to update the software of its routers. CCFF ¶ 1043.

Nor does Mr. Dooley's testimony establish LabMD's claim that "[s]ecurity risks and vulnerabilities were assessed by an outside contractor." Resp't's Post-Trial Brief at 28. Mr. Dooley testified that "we had outside contractors that were supposedly tasked with those responsibilities." CX0711 (Dooley, Dep. at 39). Mr. Dooley testified that he did not know what the outside contractors' responsibilities were. CX0711 (Dooley, Dep. at 39). He also testified that he did not interact with them much and did not know how the outside contractors assessed risks at LabMD. CX0711 (Dooley, Dep. at 39-40). Contrary to Mr. Dooley's vague recollections, the record shows that APT did not manage LabMD's security on an ongoing basis. *See supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 6-7; CCFF ¶¶ 182-190.

c. Mr. Boyle Did Not Implement Reasonable Data Security Policies, Practices, and Procedures

LabMD argues that it had good security practices in place, relying largely on Mr.Boyle's testimony. Resp't's Post-Trial Brief at 28-31. It recites in detail Mr. Boyle's prior work history in the hopes of making him appear to be an information security expert. *Id.* at 28-30. He is not. CCRRFF ¶¶ 204-206. His pre-LabMD employment establishes that he was an intermediary between IT technologists and business units wanting to use technology. Mr. Boyle was not primarily responsible for assessing the sufficiency of security built into the information technology the prior companies used, and had no hands-on experience in information security. *See* CX0704-A (Boyle, Dep. at 116-118). LabMD's reliance on Mr. Boyle to show LabMD's security was reasonable is misplaced, for a number of reasons.

First, LabMD points to Mr. Boyle's testimony that LabMD's design for transferring information within LabMD and from its clients was secure. Mr. Boyle testified that the connection was secure, but he was unable to identify the method that LabMD actually used to transfer data. CX0704-A (Boyle, Dep. at 13).

In fact, LabMD used an FTP program to transfer Personal Information from physician-clients to the Mapper server on LabMD's network. CCFF ¶¶ 84-90, 220-223. LabMD could have assured itself that its FTP transfers were reasonably secure by conducting an appropriate risk assessment to identify vulnerabilities on the network, including the FTP program and the Mapper server. *See* CCFF ¶¶ 483-496. It did not do so. LabMD's risk assessment tools were antivirus programs, firewall logs, and manual inspections, CCFF ¶¶ 524, 519, and they were either incapable of adequately assessing the range of risks that could be present on LabMD's network or were not used correctly. CCFF ¶¶ 524-609, 631-687, 691-696. Although other inexpensive or free tools were widely available to look for vulnerabilities on the FTP program

and the Mapper server, LabMD did not use them until May 2010 when it conducted a penetration test on the Mapper server. CCFF ¶¶ 514-521, 699-726. Those tests demonstrated that Mapper suffered from serious security vulnerabilities that had been publicly known for years, and could be used to take over Mapper and steal Personal Information. CCFF ¶¶ 734-743, 747, 752-808. Until 2010 when penetration testing of LabMD's servers was performed, Mr. Boyle had no basis to know whether the transfers were secure, and his testimony is simply wrong.

Second, LabMD also claims that when Mr. Boyle arrived in 2006, he found that LabMD had in place a Zywall firewall, restricted Internet access for non-managerial employees, and used the TrendMicro antivirus program, and "stratified profile setups," again suggesting that LabMD's security was reasonable. Resp't's Post-Trial Brief at 30-31, 34. Even if Respondent's citations to testimony supported the proposition – which they do not, *see* CCRRFF ¶¶ 210 – that was simply not the case. The Zywall firewall had limited logging ability and LabMD did not use the logs to assess risk, CCFF ¶¶ 637-657, and LabMD did not properly configure the firewall to block unwanted internet traffic. CCFF ¶¶ 631-648, 1075-1082, 1094-1105. As to antivirus programs, until late 2009, LabMD used the ClamWin and AVG antivirus programs on employee computers, CCFF ¶¶ 566-567, 581, 584, not TrendMicro. CX0608 (Emails between TrendMicro, Boyle, Daugherty, Kaloustian, et al.) at 2; *see* Resp't's Post-Trial Brief at 34 (asserting LabMD was using TrendMicro or Symantec). LabMD did not ensure that the ClamWin and AVG programs were working correctly on employee computers by regularly updating their virus definitions and conducting and reviewing antivirus scans on the computers. (CCFF ¶¶ 527-529, 532-536, 566-609).

Third, as to "stratified profile setups," Resp't's Post-Trial Brief at 31, which limit the ability of employees to modify computer settings, until at least November 2010, LabMD gave many, if not most, employees administrative rights over their computers, so that they had the ability to change security settings on the computers and download programs and files to the computers. CCFF ¶¶ 458-462, 880-881, 1050-1063. Again, Mr. Boyle's testimony about the adequacy of these measures, as used by LabMD, was simply wrong.

Fourth, through Mr. Boyle, LabMD suggests that its network security was managed by APT, an outside information technology vendor. However, APT did not manage or secure LabMD's internal network or assess risks and vulnerabilities on the network. CCFF ¶¶ 182-190; *supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 6-7. Its role was to install computers, connect them to networks, and respond to problems raised by LabMD employees, such as those related to internet connectivity and speed. CCFF ¶¶ 182-190. Further, in 2006 or 2007, shortly after Mr. Boyle arrived at LabMD, LabMD replaced APT with LabMD employees who were supervised by Mr. Boyle. CCFF ¶ 190.

Fifth, LabMD suggests that LabMD's walk-around inspections, some by Mr. Boyle and some by other employees, were an effective substitute for reasonable security measures that LabMD did not implement, such as penetration tests. *See* Resp't's Post-Trial Brief at 31-33. The evidence to the contrary is overwhelming. LabMD's manual inspections of employee computers for compliance with its policies were haphazard and necessarily ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696). The proof is that LabMD's manual inspections did not ever discover that LimeWire, an unauthorized application, had been installed on the Billing Computer for three years and used to share files on the P2P network. (CCFF ¶¶ 1363-1406).

Sixth, even when "LabMD established policies regarding employees' passwords and access to information," Resp't's Post-Trial Brief at 34, which was no earlier than 2010, its policies were insufficient. CCFF ¶¶ 817-821 (§ 4.4.1.1 LabMD Employees Had Access to Sensitive Information that They Did Not Need to Perform Their Jobs), ¶¶ 903-993 (§ 4.6 LabMD Did Not Require Common Authentication-Related Security Measures).

Finally, the testimony Respondent cites does not support its claim that Mr. Boyle "assumed oversight of compliance training," or that he "reviewed LabMD's processes and procedures." Resp't's Post-Trial Brief at 30-31. The evidence shows that LabMD at no point provided adequate training on security, CCFF ¶¶ 441-443, 852-900, and did not create written policies before 2010, CCFF ¶¶ 415-443, long after Mr. Boyle began to work at LabMD. *See also* JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4, Stip. 6 (stating that LabMD did not write its Policy Manual (CX0006) until 2010). Likewise, Mr. Hyer's cited testimony does not support the proposition that there were no security breaches during his tenure, or that scans were being run daily on desktops and weekly on servers. The fact that Mr. Hyer was not aware of any breaches is unsurprising and inconclusive, CX0719 (Hyer, Dep. at 156-57), as LabMD failed to use reasonable, readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities and detect security incidents. *See generally* CCFF ¶¶ 524-808 (risk assessment); *see also* CCFF ¶¶ 590-609, 626 (failed to review antivirus scans), 642-648 (failed to review firewall logs), 699-702 (did not implement an intrusion detection system or intrusion protection system), 705-712 (did not implement file integrity monitoring).

d. LabMD's Response to the Sharing of the 1718 File on a P2P Network Does Not Demonstrate that LabMD Had Reasonable Data Security Policies, Practices and Procedures

LabMD suggests that its investigation after learning that the 1718 File was being shared on a P2P network using the LimeWire application installed on the computer used by the billing manager demonstrates that its security practices were reasonable. Resp't's Post-Trial Brief at 32-33. However, LabMD admits that LimeWire was on the computer used by the billing manager for three years, JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 4, Stip. 10, indicating that it failed to implement its own putative policy relating to stratified profile users. Users without administrative access to their computers cannot download software. CCFF ¶ 1051. LabMD's internal investigation confirmed that LimeWire was installed on the billing manager's computer and that 1718 File was available for sharing. CCFF ¶¶ 1363-1372.

The investigation included a search of P2P networks for the 1718 File by a LabMD employee using her personal home computer. Resp't's Post-Trial Brief at 32; CX0730 (Simmons, Dep. at 17-18). The failure of the search to locate the 1718 File signifies nothing: the search was not exhaustive, and its failure to find the 1718 File does not indicate that the 1718 File was not then or at any time available on the P2P network. CCRRFF ¶ 227.[13] Ms. Simmons testified to searching by filename. CX0730 (Simmons, Dep. at 17-18). She did not testify to searching by file extension, hash, or using a browse host function. CCFF ¶¶ 1269-1270 (describing hash searching), ¶¶ 1284-1288 (describing file extension searching), ¶¶ 1291-1296

(describing host browsing). Furthermore, searches may sometimes fail to find files that are on the Gnutella network due to high use and network congestion, because searches only cover a portion of the network, or if the computer on which the file is located is not connected to the Internet or running a file-sharing application at the time of the search. CCFF ¶¶ 1250-1251, 1259-1266. But more tellingly about the adequacy of LabMD's security practices, as part of its investigation LabMD removed the hard drive from the billing computer and allowed it to be destroyed by an outside security firm, CCFF ¶ 1409 (citing Mr. Daugherty's deposition and trial testimony), contravening the first rule of forensic research – work with a copy of the drive and keep the original safe. Shields, Tr. 856-859.

Although Ms. Simmons testified that the billing employees were prevented from going to non-specified websites by a firewall, Resp't's Post-Trial Brief at 32, her statement is not supported by other testimony in the record. First, she testified that she did not have knowledge of the security provided by LabMD's firewall. CX0734 (Simmons, IHT at 21). Second, numerous billing employees testified that they never confirmed that any technical measures prevented them from accessing websites not needed for their jobs. In any event, Ms. Gilbreth also testified that there were no such restrictions prior to 2010. CCRRFF ¶ 225.

---

[13] The fact that Complaint Counsel did not depose Ms. Woodson is irrelevant. *See* Resp't's Post-Trial Brief at 33 n.6. Moreover, Respondent is fully aware (as it received service copies of the subpoenas) that Complaint Counsel made extensive efforts to subpoena Ms. Woodson for a deposition—through multiple attempts, by courier and process server—and that Complaint Counsel was unable to effect service by any means or at any address. On the other hand, Respondent, her former employer, failed to identify Ms. Woodson by name in its initial disclosures or provide her most recent contact information. CX0752 (Rev. Resp't's Init. Discl.).

e. LabMD Did Not Resolve Critical Risk Items Revealed By the ProviDyn Scans

Respondent's claim that starting in May 2010 it retained ProviDyn, Inc. to conduct quarterly scans, Resp't's Post-Trial Brief at 34, is not supported by the record. While LabMD retained ProviDyn in May 2010, LabMD did not retain ProviDyn to conduct quarterly scans of LabMD's servers and network. CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) does not indicate recurring scans, and Mr. Boyle's testimony does not indicate quarterly scans. In fact, the record reflects only three sets of scans conducted by ProviDyn. *See* CX0066-CX0074, CX0077-CX0084 (May 21, 2010 scans); CX0054-CX0055 (July 18, 2010 scans); CX0057-CX0065 (September 3, 2010 scans). Although these scans were conducted three months apart, there is no evidence that further scans were conducted, let alone on a quarterly basis.

Nor is Respondent's claim that LabMD resolved all of the critical risk items found in the ProviDyn scan, Resp't's Post-Trial Brief at 34, supported by the record. LabMD did not resolve all the critical risk items on the ProviDyn vulnerability scan assessments. CX0704-A (Boyle, Dep. at 37) (stating that while a resolution was defined for each vulnerability identified by ProviDyn, the resolution was not always put into place to resolve the vulnerability). In the testimony cited by Respondent, Mr. Hyer states only that a level 5 risk is a "critical risk" that "needs to be addressed right away" and said he was "sure that [he] reviewed it, resolved it," but did not provide any details. CX 0719 (Hyer, Dep. at 108 -110). The cited testimony does not indicate that risks were actually addressed. In fact, the July 18, 2010 and September 3, 2010

ProviDyn scans revealed that vulnerabilities identified in the May 21, 2010 scan were still present.[14]

Hyer's unsupported opinion that "a high priority item on the Providyn vulnerability scan assessment does not equate to a high probability of that risk actually occurring," Resp't's Post-Trial Brief at 34, is baseless and contrary to the record. The risk assessment levels in the ProviDyn reports are based on international and recognized security standards, including the PCI Security Standard and the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards and Technology (NIST). CCFF ¶ 737. A vulnerability's threat likelihood rating takes into account factors such as the ease or difficulty of exploiting the vulnerability and the impact on confidentiality, integrity, and/or availability. *See, e.g.*, CCFF ¶¶ 499-509; *see, e.g.*, CX0740 (Hill Report) at 63) (citing National Vulnerability Database, *available at* http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527). Mr. Hyer's opinion does not provide any arguments to support disregarding the expertise of these sources.

f. **LabMD's Data Security Practices in Manual Inspections, Training, and Written Policies Were Not Reasonable**

Respondent makes a number of claims relating to desktop monitoring/walkarounds, security training, and its written information security program. Resp't's Post-Trial Brief at 35-36. None of these claims are supported by the sources cited. Respondent's claim that LabMD

[14] CCFF ¶ 757 (port 21 open in all three scans, providing access to Microsoft FTP program running on Mapper server); CCFF ¶¶ 759-771 (Level 5 Anonymous FTP Writeable root Directory vulnerability, which could allow export of all the data on the Mapper server, found in May and July scans); CCFF ¶¶ 781-788 (Anonymous FTP Enabled vulnerability, which allowed a remote user without any access credentials to access any files made available on the FTP server, present on Mapper server in May and July scans); CCFF ¶¶ 792-797 (FTP Supports Clear Text Authentication vulnerability, which made usernames and passwords for the FTP application on Mapper vulnerable to sniffing by transmitting them in clear text, present on Mapper server in

employees were conducting regular desktop monitoring using a "defined LabMD checklist," Resp't's Post-Trial Brief at 35, is directly contradicted by record evidence. LabMD IT employees testified that they did not use the Walkaround Checklist, CX0482. *See* CX0730 (Simmons, Dep. at 143); CX0719 (Hyer, Dep. at 98).[15]

Nor does the record support Respondent's claim that, starting in July 2010, Mr. Boyle began conducting annual training on LabMD's Policy Manual. Resp't's Post-Trial Brief at 35. Mr. Boyle states only that LabMD created new security procedures that included "training discussions." CX0704-A (Boyle, Dep. at 68).

Furthermore, the evidence shows that neither IT nor non-IT LabMD employees received adequate security training, either before or after 2010. *See generally* CCFF ¶¶ 872-891; *see* CCFF ¶ 881 (citing testimony by post-2010 employees Bradley (CCFF ¶ 285), Brown (CCFF ¶¶ 289-290), Harris (CFF ¶ 328), and Hyer (CCFF ¶¶ 344-346)). Even had such training on LabMD's Policy Manual occurred, the policies in the Policy Manual did not describe a program for reasonable security. CCFF ¶¶ 446-455; *see also* CCRRFF ¶¶ 96-99, 111, 120-121.

Respondent relies on Mr. Maire's testimony to make several misleading statements about LabMD's security. First, while Mr. Maire does have a Bachelor's degree in Information Technology, Resp't's Post-Trial Brief at 35, he took a single wireless security class in pursuit of his degree, and did not study any other security aspects of information technology. CX0724 (Maire, Dep. at 8-9).

---

all three scans); CCFF ¶¶ 800-808 (Port 3306 found open in May and July scans, making vulnerable the database application LabMD used to store sensitive consumer information).

[15] Nor does the record support Respondent's claim that when working on LabMD computers, IT staff would check applications installed on the computer. Resp't's Post-Trial Brief at 35. For

Respondent claims that Maire's testimony shows that "LabMD had written information security policies, employee handbook, HIPAA compliance and prohibition against personal use of company equipment during his tenure." Resp't's Post-Trial Brief at 35. Mr. Maire's testimony cannot support such an inference: he did not testify that LabMD had any written information security policies other than a prohibition on use of LabMD equipment for personal use or unauthorized LabMD operations. CX0724 (Maire, Dep. at 19). Nor could Mr. Maire recall if any security topics were covered under the HIPAA guidelines. CX0724 (Maire, Dep. at 19).

Respondent next states that Mr. Maire performed daily IT rounds to check on status of all computer systems. Resp't's Post-Trial Brief at 35. While Mr. Maire did testify that he routinely checked computers, it would be incorrect to suggest that Mr. Maire performed any data security checks during his rounds. Mr. Maire's daily IT rounds involved "visit[ing] each section to query the endusers [sic] if they had an issue with any of their personal machines or a peripheral that was not known." CX0724 (Maire, Dep. at 46). If Mr. Maire was informed by a user that there was no issue with the operation of his or her computer, he would move on to the next user. CX0724 (Maire, Dep. at 48).

Respondent claims that Mr. Maire's testimony shows that LabMD had written policies related to data security, Resp't's Post-Trial Brief at 35-36, is also misleading. Contrary to Respondent's implication, the written policy cited with Mr. Maire's testimony did not exist during his tenure of May 2007 through June 2008. CCFF ¶ 357. LabMD did not create CX0006 until 2010, JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 4, Stip. 6, and Mr. Maire testified

---

example, it was not a regular event for an IT employee to look at the installed applications on a computer. CX0707 (Bureau, Dep. at 95-96).

that he only saw CX0006 as a full document after being provided it by Respondent's counsel. CX0724 (Maire, Dep. at 20). Nor does Mr. Maire's testimony suggest that he participated in implementing or enforcing these policies, or that he had any knowledge that they were implemented or enforced. Mr. Maire's role in implementing or enforcing these policies was limited to ensuring that all computers had TrendMicro installed on them. CX0724 (Maire, Dep. at 22). While Mr. Maire testified that he had "a role" in enforcing the monitoring of security software settings and applying operating system updates, CX0724 (Maire, Dep. at 24), his testimony regarding manual inspections indicates that they were performed only to troubleshoot operating issues, not to address data security vulnerabilities, and only at request of the user, CX0724 (Maire, Dep. at 45-48), not on the monthly basis as indicated by LabMD's subsequent written policy. CX0006 (Policy Manual) at 13; CCRRFF ¶ 256.

Respondent also relies on Mr. Maire for the claim that LabMD "had a firewall intrusion-prevention system in place for the period 2007-2008." Resp't's Post-Trial Brief at 36. Respondent attempts to skew Mr. Maire's words, that LabMD "had a firewall in place to prevent unauthorized intruders," CX0724 (Maire, Dep. at 91), into the proposition that LabMD implemented an intrusion protection system or intrusion detection system. Mr. Maire's testimony demonstrates he lacks the expertise to know what an intrusion prevention system is,[16] instead conflating a firewall with an IPS. *See id.* at 91-92. The evidence is clear that LabMD did not use an intrusion detection system or intrusion protection system. CCFF ¶¶ 699-702.

Finally, the fact that "Maire was not aware of any breach or occurrence of access to information by individuals not authorized to access such information," Resp't's Post-Trial Brief

[16] Complaint Counsel provided evidence on Intrusion Detection Systems; "intrusion prevention system" is the term Mr. Maire uses. CCFF ¶¶ 699-702.

at 36, is unsurprising, irrelevant, and misleading. It is unsurprising because there is no reason to think Mr. Maire would be aware of any breach or unauthorized access to information; Mr. Maire did not have data security responsibilities at LabMD. CCRRFF ¶ 154. It is irrelevant because, given his lack of responsibilities in this area, the fact that he did not know of any breaches would not indicate that they had not occurred. And it is misleading because Mr. Maire was aware of the sharing of the 1718 File on a P2P network. CX0724 (Maire, Dep. at 64).

B. Mr. Fisk's Testimony Does Not Establish That LabMD Had Reasonable Data Security

Respondent's reliance on Mr. Fisk's report to support a conclusion that LabMD's security was not only reasonable but constituted best practices is untenable. As an initial matter, Respondent's brief cites to Mr. Fisk, and *only* to Mr. Fisk, to establish such factual propositions as: LabMD had two layers of properly configured firewalls, user profiles limited the ability of non-managers to download files from the Internet and install applications, the Cisco 1841 router as deployed by LabMD had both firewall and intrusion prevention capabilities, and LabMD regularly checked employee machines to ensure employees did not violate LabMD's policy against installing applications. Resp't's Post-Trial Brief at 36.[17] To the extent that Respondent relies on Mr. Fisk's opinion alone to establish facts in this case, Respondent's brief is in violation of the Court's Order on Post-Trial Briefs, which reiterates that factual propositions should be established by fact witnesses or documents. Order on Post-Trial Briefs at 2 (July 16, 2015).

[17] In Respondents reply brief, RX533 is identified as a deposition. RX533 is Mr. Fisk's report and the citations appear to refer to his report.

Even if Mr. Fisk's testimony could establish the security measures LabMD deployed, Mr. Fisk does not have any experience that suggests that he is qualified to evaluate the reasonableness of a company's overall security posture. CCRRFF ¶ 278. Mr. Fisk's experience is devoted solely to the development of P2P software. RX533 (Expert Report of Adam Fisk) at 35 (describing Mr. Fisk's experience from 2000 to the present); Fisk, Tr. 1175-1177 (admitting that he testified at his deposition that he had never evaluated a company's data security). The overwhelming evidence contradicts Mr. Fisk's claim LabMD could meet "a best practices standard," Resp't's Post-Trial Brief at 36, by merely having firewalls and profiles that prevented non-managers from downloading files and installing apps is contradicted by overwhelming evidence. Complaint Counsel has shown that such superficial and isolated measures cannot constitute reasonable security practice. *See, e.g.*, CCFF ¶¶ 384-395, 524; CCCL ¶¶ 15-20.

Further, LabMD failed to meet even the minimal standard that Mr. Fisk suggests. First, there is no evidence to support Mr. Fisk's assertion that LabMD had two layers of properly configured firewalls. Mr. Fisk bases his assertion on the fact that the router used by LabMD had firewall capabilities and his assumption that those capabilities were probably activated.[18] RX533 (Expert Report of Adam Fisk) at 20-21. In fact, the router's firewall capabilities were not activated. CCFF ¶ 1086. Mr. Fisk's assertion that LabMD's firewalls were properly configured is equally erroneous. LabMD did not properly configure its firewall to block IP addresses and unnecessary ports. CCFF ¶¶ 1094-1105.

---

[18] As noted above, to the extent that Respondents are relying on Mr. Fisk's opinion to establish the fact that the router's firewall capabilities were activated, this is in violation of the Court's Order on Post-Trial Briefs because it cites an opinion by Respondent's expert to support factual propositions that should be established by fact witnesses or documents. Order on Post-Trial Briefs at 2 (July 16, 2015).

Second, LabMD did not, as Mr. Fisk suggests, properly employ profiles that prevented employees from downloading files or installing apps. CCFF ¶¶ 460-61, 1056-1060. Until at least 2010, many LabMD employees, including some non-managers, had administrative rights to their computers and unrestricted access to the internet. CCFF ¶¶ 460-61, 1056-1060.

Mr. Fisk's claim that LabMD's manual examinations of employee workstations effectively compensated for LabMD's failure to deploy file integrity monitoring is also incorrect. Manual inspections as performed by LabMD were an ineffective security measure because they could not reliably detect threats and were not regularly performed. *See* CCFF ¶¶ 660-664 (manual inspections could not reliably detect security risks), 668-677 (LabMD performed manual inspections only on request when employee workstations malfunctioned), 680-685 (LabMD did not provide guidance for manual inspections until 2010), 691-696 (LabMD's manual inspections did not detect LimeWire), 708 (manual inspections are less effective and less efficient than file integrity monitoring).

Respondent also misrepresents Mr. Fisk's claim about best practices and file integrity monitoring. Resp't's Post-Trial Brief at 36-37. Mr. Fisk did not state that "[t]he best practices guidelines during the Relevant Period did not include File Integrity Monitoring in their recommendations." *Id.* at 37. Instead, he stated that file integrity monitoring was not included in the "best practices guidelines reviewed for this report." RX533 (Expert Report of Adam Fisk) at 33. Mr. Fisk's limited expertise in information security is not sufficient to determine the relevant best practices at the time. CCRRFF ¶¶ 275, 278. In any event, these documents cannot support a claim that – for a business maintaining hundreds of thousands of consumers' sensitive personal information, including health information – file integrity monitoring could not be a component of reasonable data security practices.

Finally, Mr. Fisk's statement that the 1718 File could have been obtained even through a properly configured firewall, Resp't's Post-Trial Brief at 37, is irrelevant. LimeWire permits users to obtain documents from computers that are behind a firewall using an outbound connection to an ultrapeer, so the presence of a firewall on LabMD's system did nothing to prevent the removal of the 1718 file. *See* CCFF ¶¶ 1234-37. Even if Mr. Fisk's statement was relevant, it is inaccurate because LabMD's firewall was not properly configured. CCFF ¶¶ 1094-1105.

III. Day Sheets

In its discussion of the Sacramento incident, LabMD confirms the heart of Complaint Counsel's allegation: that the Sacramento Police Department found copies of LabMD Day Sheets and copies of checks containing consumers' Personal Information in the possession of individuals unrelated to LabMD. Resp't's Post-Trial Brief at 37.

However, LabMD falsely states that Day Sheets were not saved electronically. Resp't's Post-Trial Brief at 38. Some of LabMD's Day Sheets, which it retained indefinitely in paper form, CCFF ¶ 160, were scanned and saved to LabMD's computer network as part of an archive project by the company, CX0733 (Boyle, IHT at 37, 46-47), and billing employees had the option of saving Day Sheets electronically to a computer. CX0714-A ([Fmr. LabMD Empl.], Dep. at 60-61). Respondent also mischaracterizes Professor Hill's testimony about LabMD's physical security. Dr. Hill's evaluation of LabMD's physical security was limited to LabMD's provision of locks to server rooms and physical access to LabMD computers. Hill, Tr. 293. Dr. Hill did not address LabMD's practice of storing Day Sheets in unlocked storage rooms, or in filing cabinets that could be accessed by anyone who came into the Billing Department with no measures to physically stop someone from accessing them. CCFF ¶¶ 157-159.

While there is no conclusive explanation of how LabMD Day Sheets were exposed, the fact that they were discovered in identity thieves' possession demonstrates that leaks of LabMD's sensitive data and the resulting consumer injury are ongoing concerns. Further, proof of a data breach is not a requirement for LabMD's practices to be unfair in violation of Section 5. *See* Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 96; Burden of Proof, § II (Section 5(n) Sets Forth Complaint Counsel's Burden of Proof on Injury), at 46-47; CCCL ¶ 24; CCRRCL ¶ 77.

IV. Respondent Has Offered No Legal Argument Precluding Entry of the Notice Order in this Proceeding

Respondent recites a number of conclusory statements, without any citation to legal authority or record evidence, under the heading "Predicates to Relief." Resp't's Post-Trial Brief at 38-39. Each of these arguments is addressed elsewhere in this Reply Brief or below. Complaint Counsel addresses Respondent's argument regarding the harm LabMD caused or likely caused to consumers *infra*, Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 95-98. Complaint Counsel addresses Respondent's novel and legally unsupported claim that Complaint Counsel must prove LabMD's unfair acts or practices are likely to recur *infra*, Burden of Proof, § I (Complaint Counsel's Burden of Proof is Defined by Section 5), at 42-43.[19] Complaint Counsel addresses Respondent's unavailing argument that Section 5's unfairness standard is different for the medical industry *infra*, Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41. Complaint Counsel addresses Respondent's unsupported claim that it relied on IT professionals and outside experts *infra*, Argument, § II.C.4 (LabMD

Had Control Over and Was Responsible For its Own Unreasonable Data Security), at 131-33; *see also supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 5-8. Respondent offers no evidence that its system was proven effective and useful by its physician-clients, and points to nothing in the record to indicate that no physician-client ever complained of a patient's identity theft, medical identity theft, or HIPAA violations. Finally, Complaint Counsel demonstrates that it has proven LabMD's Section 5 violations were serious and warrant fencing-in relief *infra*, Argument, § II.D. (Entry of the Notice Order is Appropriate and Necessary) at 141-45. And while Complaint Counsel agrees that there is no evidence of prior violations of the FTC Act by LabMD, this is no way makes fencing-in relief inappropriate here. *See* CCRRCL ¶ 231.

BURDEN OF PROOF/STANDARD OF REVIEW

Complaint Counsel has the burden of proving that LabMD violated Section 5 by a preponderance of the evidence, CCCL ¶ 1-3, which it has done. Not content with Complaint Counsel's burden, Respondent attempts to break down Section 5 to its component words and apply an out-of-context common meaning analysis to each individual word in order to apply limitations to Section 5's unfairness provision that are not supported either by the statute or by case law. *See* Resp't's Post-Trial Brief at 39-41, 65. Section 5(n) defines an unfair practice as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n); *see also* JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 2 (joint stipulation of law accepting this definition of an unfair practice.) This test has been

---

[19] To the extent Respondent's claim relates to relief, it is addressed *infra*, Argument, § II.D (Entry of the Notice Order is Appropriate and Necessary), at 141-45.

recognized as "the most precise definition of unfairness articulated by either the Commission or Congress." *Am. Fin. Servs. Assoc. v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985); *see also* CCRRCL ¶ 51.

Respondent's contention that the common meaning of the terms in Section 5 is the only criteria for interpreting its meaning is erroneous. *See* CCRRCL ¶ 51. "Whether a statutory term is unambiguous . . . does not turn solely on dictionary definitions of its component words." *Yates v. U.S.*, 135 S.Ct. 1074, 1081 (2015). Where, as here, the statute provides a definition and sufficient context for understanding a term, it is not necessary to resort to a dictionary definition. *See, e.g.*, *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.' (citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 240 (1989))); *see also* Comm'n Order Denying Resp't's Mot. to Dismiss at 16 (Jan. 16, 2014) ("[T]he three-part statutory standard governing whether an act or practices is 'unfair' set forth in Section 5(n) . . . is sufficient to give fair notice of what conduct is prohibited.").

Respondent's attempt to use general policy statements about the FTC's authority in order to summon a requirement that Complaint Counsel must prove that LabMD's conduct has "a generalized, adverse impact on competition or consumers," or a connection to the "protection of free and fair competition in the Nation's markets," Resp't's Post-Trial Brief at 40-41, is without merit or support. *See* CCRRCL ¶ 47. There is no such requirement to be found in the statute, nor has any court ever required such a proof. The Commission defined unfairness in a 1980 policy statement. *Policy Statement on Unfairness* (Dec. 17, 1980), appended to 104 F.T.C. 949, 1984 WL 565290 (Unfairness Statement). In 1994, Congress codified the Unfairness Statement in Section 5(n) of the FTC Act. *See* H.R. Rep. 103-617 at 12 (1994). By adopting the

Unfairness Statement, Congress decided to constrain the Commission's unfairness authority with—and *only* with—the limitations set forth in Section 5(n). Respondent admits that "Section 5(n) . . . controls here." Resp't's Post-Trial Brief at 69-70. Congress, courts, and the Commission have applied Section 5 to unfair practices for decades and none has ever suggested that the term should be limited as Respondent proposes.

Further, Respondent's appeal to general statutory interpretation techniques, *see, e.g.*, *Yates*, 135 S. Ct. at 1082-83, 1085, and speeches *see, e.g.*, J. Howard Beales, Former Dir., Fed. Trade Comm'n, Speech: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection, at § II (May 30, 2003), cannot introduce entirely new requirements that are not suggested by the language of the statute. *See Am. Fin. Servs.*, 767 F.2d at 972. Respondent's attempt to add limitations to the plain language of the statute is erroneous and without legal authority. *See Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'" (citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 240 (1989))).

I. Complaint Counsel's Burden of Proof is Defined by Section 5[20]

Respondent attempts to contort Section 5 beyond recognition, arguing for new interpretations of long-established terms and new statutory elements.

First, Respondent argues that a case involving past acts or practices requires Complaint Counsel to prove such acts are likely to recur and that such recurrence is likely to cause injury in the future. Resp't's Post-Trial Brief at 42. Section 5(n) on its face does not require that Complaint Counsel prove by a preponderance of the evidence that a challenged act or practice is

[20] Respondent's Corresponding heading for this section is "Causation." Resp't's Post-Trial Brief at 42.

likely to recur. 15 U.S.C. § 45(n). Respondent's claims regarding the likelihood of recurrence misstates the law, and its reliance on *Borg-Warner Corp. v. FTC*, 746 F.2d 108 (2d Cir. 1984), is misplaced. In *Borg-Warner*, the Second Circuit explicitly declined to review the Commission's "substantive legal rulings," *i.e.*, its determination that the conduct at issue in the case had violated the law, and reviewed only the appropriateness of injunctive relief as a remedy. *Id.* at 110. *Borg-Warner* did not add a new element of proof to Section 5 violations.

To the extent Respondent is attempting to argue that injunctive relief is inappropriate on the basis of *Borg-Warner*, the violations in that case were not "flagrant or longstanding." *Id*. at 111. The court determined the petitioner was completely out of the industry alleged to have violated the law and had stopped the alleged conduct long before the Commission decided the case. *Id*. at 110. In this case, however, the evidence shows that LabMD has a long history of failing to provide reasonable data security for the Personal Information it maintains, CCFF ¶¶ 382-1110, has no intent to dissolve as a Georgia corporation, JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 3, and intends to employ the same policies and procedures to information in its possession as it employed in the past. CX0765 (LabMD's Resps. to Second Set of Discovery) at 5-6 (Resp. to Req. 38), 7 (Resp. to Interrog. 12). As the *Borg-Warner* court recognized, "[t]he appropriateness of injunctive relief necessarily varies from case to case, and relatively slight factual differences may justify different treatment. *Borg-Warner*, 746 F.2d at 111.

After a violation has been proven, it is Respondent – not Complaint Counsel – that bears a heavy burden to prove that no permanent injunction is warranted because there is "no reasonable expectation" of future repetitions of the wrongful conduct. *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 632-33 (1953); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 190 (2000) (Respondent bears the "formidable burden of showing that it is

absolutely clear the allegedly wrongful behavior could not reasonably be expected to recur."); CCCL ¶¶ 60-69. Past illegal conduct is highly suggestive of the likelihood of future violations. *FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 536 (S.D.N.Y. 2000) (citing *SEC v. Mgmt. Dynamics, Inc.*, 515 F.2d 801, 807 (2d Cir. 1975)); *FTC v. U.S. Oil and Gas Corp.*, No. 83-1702-CIV-WMH, 1987 U.S. Dist. LEXIS 16137, at *51 (S.D. Fla. July 10, 1987). Respondent's use of dictionary definitions does not change the clear authority that Respondent must prove no reasonable expectation of repeating the same conduct. *See* Burden of Proof/Standard of Review, at 39-41, *supra*. The evidentiary record establishes that Respondent intends to continue to operate and follow the same practices in the future. *Infra* Argument, § II. D (Entry of the Notice Order is Appropriate and Necessary) at 142-43; CCCL ¶¶ 60-69, 112-114.

Second, the Commission has interpreted Section 5 to apply in this case where LabMD's actions "caused or likely caused consumer injury," contrary to Respondent's reliance on verb tense. Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014) (holding that the complaint alleges harm because "actual and potential data breaches it attributes to LabMD's data security practices caused or were likely to cause cognizable, 'substantial injury' to consumers"). Even if that were not the case, the disclosures of Personal Information held by LabMD are likely to cause consumer harm in the future. CCCL ¶¶ 24-27; *see, e.g.*, CCFF ¶¶ 1661-1770 (analyzing likely harm to consumers from the 1718 File and the Sacramento Day Sheets). To the extent Respondent's argument relates to the appropriateness of entry of the notice order, Complaint Counsel has proven that there is "some cognizable danger of recurrent violation." *FTC v. Accusearch*, 570 F.3d 1187, 1201 (10th Cir. 2009) (quoting *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)); *see* CCCL ¶¶ 57-71.

Third, Respondent uses various dictionary definitions of the term "likely" to try to expand Section 5(n)'s requirements. This technique is without merit. First, as discussed above, Respondent's appeals to dictionary definitions cannot overcome the clear language of the requirements set forth in Section 5(n). *See Robinson*, 519 U.S. at 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'" (citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 240 (1989))). Second, to the extent that dictionary definitions are even relevant, Respondent cannot cherry-pick one dictionary definition to suit its purpose. Indeed, another dictionary definition of the term "likely" includes "seeming to be true" (Merriam-Webster). Thus, there is no basis to introduce heightened standards for the term "likely."

Finally, Respondent makes a number of claims that have been addressed elsewhere. Respondent claims that Complaint Counsel must show that LabMD's data security practices departed from medical industry standards. Resp't's Post-Trial Brief at 43. Respondent also claims Complaint Counsel must show that LabMD's reliance on its IT professionals was unreasonable. These claims are addressed *infra*. *See* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41; Argument, § II.C.4 (LabMD Had Control Over and Was Responsible For its Own Unreasonable Data Security), at 131-33; *see also supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 5-8.

Respondent also claims that Complaint Counsel must prove "LabMD's data security practices alleged to have been unfair in the complaint (a) cause or, (b) such practices are either (i) probable or highly probable to re-occur (the Section 5(n) plain language standard) or (ii) a "cognizant danger" – that is, something more than a conjectural or speculative danger – to re-occur (the pre-Section 5(n) case law standard), and "likely to cause" an actual data breach in the

future." Resp't's Post-Trial Brief at 43. In fact, as set forth in Section 5(n) and discussed above, Complaint Counsel must prove only that LabMD's practices are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. *See* CCCL ¶ 3; JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 3); Comm'n Order Denying Resp't's Mot. to Dismiss at 18-19 (Jan. 16, 2014).

II. Section 5(n) Sets Forth Complaint Counsel's Burden of Proof on Injury

Complaint Counsel's burden of proof is well-established, and Respondent's repeated attempts to add to it must fail. Complaint Counsel must prove that LabMD's acts or practices caused or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not offset by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n); *see also* CCCL ¶ 3; JX0001-A (Joint Stips. Of Fact, Law, and Auth.) at 3.

As to the injury prong, contrary to Respondent's misrepresentation, *see* Resp't's Post-Trial Brief at 44, "occurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted unfair . . . acts or practices." Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014) (internal citations and quotations omitted); *see also FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *6 (3d Cir. Aug. 24, 2015) ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."). The Commission's Unfairness Statement does not support a different rule. *See* Resp't's Post-Trial Brief at 44 n.8. Although the Unfairness Statement contemplates that substantial injury "[i]n most cases . . . involves monetary harm," it also notes that "[u]nwarranted health and safety risks" can support unfairness. *Int'l Harvester*

Co., Docket No. 9147, 104 F.T.C. 949, 1984 WL 565290, at *97 (1984) (unfairness statement). Moreover, the Unfairness Statement states that a practice can be unfair if it causes "a small harm to a large number of people, or if it raises a significant risk of concrete harm." *Id.* at *97 n.12. Therefore an "actual data security breach" is not required for a practice to cause or be likely to cause substantial injury to consumers. Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014).[21]

As to the second and third prongs of Section 5(n), the Unfairness Statement, which Respondent quotes without citation, *see* Resp't's Post-Trial Brief at 45, does not supplement or alter the burden of proof. *See* CCRRCL ¶ 47. The Unfairness Statement observes that many unfairness matters are brought based on "certain types of sales techniques," and that, in such cases, the action is brought "to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking." *Int'l Harvester Co.*, Docket No. 9147, 104 F.T.C. 949, 1984 WL 565290, at *97 (1984) (Unfairness Statement). This specific example of how the Commission would have applied the unfairness doctrine in a sales technique case does not limit the Commission's authority in a case such as this one, which does not involve sales techniques.

Even if the specific example did apply, the evidence proves that consumers could not exercise free decision-making with regard to LabMD's security practices because they had no way of knowing that LabMD would receive their specimen and Personal Information, and had no

---

[21] In addition, Respondent cannot prevail on an argument that the Security Incidents alleged in the Complaint are not "actual data breaches." The unauthorized disclosure of thousands of consumers' sensitive personal information by LabMD would satisfy any definition. The uncontroverted evidence shows that the LimeWire was installed on the Billing Computer, the 1718 File was available on a P2P network, and the 1718 File was found and downloaded on the P2P network using an off-the-shelf P2P client, such as LimeWire. CCFF ¶¶ 1363-1396.

way of knowing LabMD's unreasonable security practices. *See Orkin Exterminating Co. v. F.T.C.*, 849 F.2d 1354, 1365 (11th Cir. 1988); CCFF ¶¶ 1777-1787. And where consumers do not knowingly purchase a product or service, there are unlikely to be countervailing benefits to a company's unfair practices. *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (finding no countervailing benefits where consumers "did not give their consent to enrollment in OnlineSupplier, and thus, the harm resulted from a practice for which they did not bargain."); *see also* CCCL ¶¶ 42-44.

Finally, Complaint Counsel addresses elsewhere in this brief Respondent's assertion that Complaint Counsel must prove that LabMD's security practices were unreasonable for medical companies during the relevant time period. *See* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

III. Complaint Counsel's Burden of Proof is Preponderance of the Evidence

Respondent's argument that one dictionary's definition of "likely" as "having a high probability of occurring" somehow transforms the burden of proof in this case from the preponderance of the evidence standard to the clear and convincing standard, Resp't's Post-Trial Brief at 42-43, 45-46, contradicts clearly established law and Respondent's own stipulations in this case. *See* CCRRCL ¶ ¶ 61-64; JX0001-A (Joint Stips. Of Fact, Law, & Auth.) at 2-3).

The proper standard of proof in unfairness cases is preponderance of the evidence.[22] CCCL ¶ 2; JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2-3). Complaint Counsel must prove, by preponderance of the evidence, that consumer injury is likely. CCCL ¶ 3; JX0001-A

[22] Respondent also argues that Complaint Counsel may not carry its burden using illegally obtained evidence. Resp't's Post-Trial Brief at 46. No evidence in this proceeding was obtained illegally, as discussed *infra*, Argument, § 1.C.2 (LabMD's Due Process Rights Under the Fourth Amendment Have Not Been Violated in This Proceeding) at 71 n.36.

(Joint Stips. of Fact, Law, & Auth.) at 2-3). None of the authorities that Respondent cites suggest that the term "likely" means that clear and convincing evidence is required. In *Colorado v. New Mexico*, 467 U.S. 310, 315-17 (1984), the Court applied the heightened standard of proof to a hearing by a Special Master to equitably apportion the waters of the Vermejo River between Colorado and New Mexico. The Court applied this heightened standard based on "the unique interests involved in water rights disputes between sovereigns," not because any statute involved required showing that any event was "likely." *Colorado*, 47 U.S. at 315-16. The case referred to the language "highly probable" only to the extent that the Court had used it in a previous proceeding in directing that a diversion of interstate water should be allowed only if Colorado, the state with the burden of proof, could "place in the ultimate factfinder an abiding conviction that the truth of its factual contentions are 'highly probable." *Id.* at 316. (Citations omitted). This has no relevance to the statutory definition found in Section 5(n). Respondents have presented no authority that supports the extraordinary claim that the word "likely" in a statute raises the burden of proof beyond preponderance of the evidence.

ARGUMENT

I. This Proceeding Does Not Violate Any Constitutional or Statutory Provisions

A. The FTC's Administrative Law Judges Are Not Appointed in Violation of the Constitution

1. Respondent's Sixth Affirmative Defense Should Be Denied.

Respondent's Sixth Affirmative Defense, which asserts that FTC ALJs are improperly appointed under the Constitution's Appointments Clause and that their tenure protections violate the Constitution's separation of powers, is without merit and Respondent's request for dismissal should therefore be denied. *See* Resp't's Post-Trial Brief at 47-48 (asserting that FTC ALJs' adjudicatory functions make them Inferior Officers under the Constitution); *see also* First

Amended Ans. at 6. The Appointments Clause provides, in pertinent part, that the President, with the advice and consent of the Senate, shall select principal officers of the United States (*e.g.*, Secretary of State, Secretary of Defense, *etc.*), and that:

> all other Officers of the United States, whose Appointments are not herein otherwise provided for, and which shall be established by Law: but the Congress may by Law vest the Appointment of such inferior Officers, as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments.

U.S. CONST. Art. 2, § 2, cl. 2.

The Appointments Clause, however, has no applicability here because FTC ALJs are civil service employees, and not "inferior Officers" under the Constitution. *See Buckley v. Valeo*, 424 U.S. 1, 126, n. 162 (1976) (Appointments Clause does not reach government personnel below Inferior Officers); *Tucker v. Comm'r of Internal Revenue*, 676 F.3d 1129, 1132 (D.C. Cir. 2012) (same). Furthermore, even assuming that FTC ALJs are deemed to be Inferior Officers, the relevant statutory and regulatory authority providing for the appointment of FTC ALJs satisfy the Appointments Clause and the ALJs' tenure protections are constitutionally appropriate. Finally, even assuming *arguendo* an Appointments Clause violation, such violation would not vitiate, in whole or in part, Respondent's liability under the FTC Act. Accordingly, Respondent's Sixth Affirmative Defense should be rejected.

a. **FTC ALJs Are Not Inferior Officers**

As recognized by the Supreme Court, the vast majority of government personnel are employees, or "lesser functionaries subordinate to officers of the United States." *See Buckley*, 424 U.S. at 125-26, n.162; *see also Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 506, n.9 (2010); *U.S. v. Germaine*, 99 U.S. 508, 509 (1879). Inferior Officers under the Constitution are only those "appointee[s] exercising significant authority pursuant to the laws

of the United States." *Buckley*, 424 U.S. at 126. FTC ALJs do not meet this standard because they have limited functions, are subject to the Commission's plenary authority, and do not issue final decisions. Indeed, this finding is confirmed by Congress' long-standing treatment of ALJs as employees.

Congress gave the Commission the authority to employ ALJs in its discretion, and if so, decide which specific functions to delegate to them, if any. *See* 5 U.S.C. § 3105; 26 Fed. Reg. 6191 at §1a, 75 Stat. 837 (Eff. July 9, 1961) (Reorganization Plan No. 4 of 1961). The Commission has retained the sole authority to issue complaints, decide in the first instance all dispositive motions to dismiss and motions for summary judgment, accept any settlements and issue consent orders, and to issue the final decisions and orders regarding potential FTC Act violations and any resulting remedies. *See* 16 C.F.R. §§ 3.11(a), 3.22(a), 3.25(f), & 3.54. The Commission has delegated certain lesser functions to its ALJs. *See* 16 C.F.R. § 3.42(c).

These delegated functions do not transform FTC ALJs from valued government employees to Inferior Officers under the Constitution.[23] For example, certain responsibilities, such as issuing subpoenas and taking depositions, can also be performed by privately employed counsel representing respondents. *See* 16 C.F.R. §§ 3.33(a) & 3.34(a-b). Indeed, while the ALJ may issue subpoenas or discovery orders, he cannot force a non-complying party to produce evidence that it is wrongfully withholding; rather, an ALJ can only "certify to the Commission a request that court enforcement of the subpoena or order be sought." *See* 16 C.F.R. § 3.38(c).

---

[23]Although ALJs are not Inferior Officers under the Constitution, they are like many other Commission employees who play a vital role in the efficient functioning of the FTC: the Commission can more readily fulfill its mission to protect consumers and competition because ALJs preside over time-staking enforcement hearings and focus the legal issues and relevant evidence for Commission review.

Likewise, the ALJ's ministerial functions, such as rejecting submissions that do not comply with the rules, do not represent the exercise of "significant authority pursuant to the laws of the United States." *See Freytag v. Comm'r of Internal Revenue*, 501 U.S. 868, 881 (1991) (finding Special Trial Judges to be Inferior Officers in part because they perform more than ministerial functions).

The FTC ALJs' more substantive responsibilities also do not elevate them above mere government employees to Inferior Officers because their actions are subject to the plenary review of the Commission. For example, while the ALJ may receive evidence and make evidentiary rulings in accord with very specific Commission rules, *see* 16 C.F.R. §§ 3.31-3.46, any excluded evidence (including any proffers) is retained in the record and available for any reviewing authority, and the Commission may reopen the proceedings for additional evidence if it deems it necessary. *See* 16 C.F.R. §§ 3.43(h)(1), 3.54(c) & 3.71; *see also* 16 C.F.R. § 3.23(b) (providing for interlocutory review by Commission of certain ALJ rulings if significant to case).

Most significantly, the ALJs' Initial Decisions are not final orders of the Commission, and such decisions are not afforded any deference by the Commission in its plenary review. *See* 16 C.F.R. §§ 3.51(b) ("An initial decision shall not be considered final agency action subject to judicial review under 5 U.S.C. 704."), 3.52(a) (Commission review of Initial Decision automatic without appeal when preliminary injunction sought in federal court), 3.53 (Commission review of Initial Decision in absence of appeal), & 3.54(b) (Commission may adopt, modify or set aside any finding in the Initial Decision). When reviewing the ALJ's Initial Decision, the Commission applies a *de novo* standard of review to all of the ALJ's findings of facts, including factual findings "based on the demeanor of a witness" and inferences drawn from those facts, and his

conclusions of law. *Realcomp II Ltd.*, Dkt. No. 9320, 2007 WL 6936319, at *16 n.11 (F.T.C. Oct. 30, 2009), *aff'd*, 635 F.3d 815 (6th Cir. 2011).

The D.C. Circuit has found this lack of final decision-making authority to be the "critical" factor in determining whether federal government personnel are mere employees or Inferior Officers under the Constitution. *See Landry v. FDIC*, 204 F.3d 1125, 1133-34 (D.C. Cir. 2000). In *Landry*,[24] the D.C. Circuit found that FDIC ALJs are not Inferior Officers because they do not have the power to issue final decisions, even though they exercise "significant discretion" when they "take testimony, conduct trials, rule on the admissibility of evidence, and have the power to enforce compliance with discovery orders." *Id.* (interpreting Supreme Court's *Freytag* decision as laying "exceptional stress" on the final decision-making power of the Tax Court's Special Trial Judges when finding them to be Inferior Officers); *cf. Freytag*, 501 U.S. at 880, 891 (finding Special Trial Judges to be Inferior Officers in part because they had power "to grant certain injunctive relief" and "to order the Secretary of the Treasury to provide a refund of an overpayment determined by the [Special Trial Judge]," and because their judgments were only appealable under a deferential review standard).

Congress' treatment of FTC ALJs (or their precursor, hearing examiners) confirms that FTC ALJs are mere employees and not Inferior Officers. *See Weiss v. U.S.*, 510 U.S. 163, 194 (1994) (Souter, J., concurring) ("in the presence of doubt" as to whether military judges were principal or inferior officers, "deference to the political branches' judgment is appropriate"). Congress is presumed to know the requirements of the Appointments Clause, *see Cannon v. Univ. of Chicago*, 441 U.S. 677, 696-97 (1979), and it specified in the FTC Act that,

---

[24]The D.C. Circuit in *Landry* is the only Court of Appeals that has considered the question of whether any agency ALJ is an Inferior Officer under the Constitution.

> *The commission shall appoint a secretary*, who shall receive a salary, and it *shall have authority to employ and fix the compensation of such attorneys, special experts, examiners, clerks, and other employees* as it may from time to time find necessary for the proper performance of its duties and as may be from time to time appropriated for by Congress.

15 U.S.C. § 42 (emphasis added). Likewise, Congress specifically stated that ALJs shall be appointed by the relevant "agency," and not the President, Head of Department, or Judiciary. *See* 5 U.S.C. § 3105; *see also Ramspeck v. Fed. Trial Exam'rs Conference*, 345 U.S. 128, 133 (1953) (finding "position of hearing examiners is not a constitutionally protected position," and that Congress intended for the compensation, promotion and tenure of hearing examiners (the precursor to modern-day ALJs) to be independent of their agency, but "were specifically declared to be otherwise under the other provisions" of the competitive service regulations).

Because FTC ALJs are not Inferior Officers under the Constitution, the Appointments Clause does not apply to them and Respondent's Sixth Affirmative Defense should be denied.

b. Relevant Statutory and Regulatory Authority Providing for the Appointment of FTC ALJs Satisfy the Appointments Clause

Even assuming *arguendo* that FTC ALJs are Inferior Officers, the relevant statutory and regulatory authority relating to the appointment of FTC ALJs satisfies the requirements of the Appointments Clause. *See* U.S. CONST. Art. 2, § 2, cl. 2 (Inferior Officers shall be appointed by "the President alone, in the Courts of Law, or in the Heads of Departments"). Respondent incorrectly asserts that FTC ALJs are appointed by the Office of Personnel Management (OPM). Resp't's Post Trial Brief at 47 (citing FTC regulation and website). FTC ALJs, however, are not appointed *by* OPM, but "under the authority of" OPM. *See* https://www.ftc.gov/about-

ftc/bureaus-offices/office-administrative-law-judges ("Administrative Law Judges are independent decision makers, appointed *under the authority of* the Office of Personnel Management.") (emphasis added); 16 C.F.R. § 0.14 (same). This is a critical distinction. While OPM can, among other things, recruit ALJ applicants and develop and administer the examinations used to qualify for the position, OPM does not have the authority to appoint ALJs for the FTC or agencies like the FTC. *See* 5 C.F.R. § 930.201(e).

Instead, the Commission selects and appoints its ALJs from a "list of eligibles" provided by OPM. *See* 5 C.F.R. § 930.204(a) ("An agency [including the FTC] may appoint an individual to an administrative law judge position only with prior approval of OPM, except when it makes its selection from the list of eligibles provided by OPM."). Under the Reorganization Plan No. 8 of 1950, the President specified that appointments of major administrative departments by the FTC Chairman shall be subject to the approval of the full Commission, and Commission regulations set forth the office of ALJs as a principle unit of the Commission. Reorganization Plan No. 8 of 1950, 15 Fed. Reg. 3175, at § 1b(2), 64 Stat. 1264 (Eff. May 24, 1950) ("The appointment by the Chairman of the heads of major administrative units under the Commission shall be subject to the approval of the Commission."); 16 C.F.R. § 0.9 (listing "Office of the Administrative Law Judges" as "principal unit" of the Commission).

Thus, even assuming that FTC ALJs are Inferior Officers, the relevant statutory and regulatory authority relating to the appointment of FTC ALJs satisfies the requirements of the Appointments Clause. Because Respondent has therefore not proven an Appointments Clause violation, this Court should deny Respondent's Sixth Affirmative Defense.

c. FTC ALJs' Tenure Protections are Constitutional

Respondent also challenges an FTC ALJ's tenure protections under the guise of its Sixth Affirmative Defense. *See* Resp't's Post-Trial Brief at 47-48. This challenge should be denied because Respondent's Answer did not provide notice of this new challenge because it only challenged the manner of the FTC ALJs' appointments, not their tenure protections. *See* Amended Ans. at 6 ("The claims alleged in the Complaint are barred, in whole or in part, because this administrative proceeding violates Article II of the United States Constitution because the presiding Administrative Law Judge is an "inferior officer" for Article II's purposes but was not appointed by the Commissioners, the President, or the Judiciary."); 16 C.F.R. § 3.12(b)(1)(i) (answers "shall" contain a "concise statement of the facts constituting each ground of defense"). This challenge should also be denied because FTC ALJs are not Inferior Officers. *See, supra,* Argument, § I.A.1.1 (FTC ALJs Are Not Inferior Officers), at 50-54; *see also Buckley*, 424 U.S. at 126, n. 162. Even assuming *arguendo* that FTC ALJs are Inferior Officers, this challenge should be denied on the merits.

The Constitution allows Congress to place restrictions on the removal of Inferior Officers provided that the restrictions do not unduly interfere with the President's exercise of Executive power. *See, e.g., Free Enterprise,* 561 U.S. at 483, 498; *Humphrey's Executor v. United States*, 295 U.S. 602, 631-32 (1935); *U.S. v. Perkins*, 116 US 483, 485 (1886). Courts decide the constitutionality of such restrictions on a case-by-case basis, and such decisions "depend upon the character of the office" at issue and whether such restrictions would interfere with the President's duty to "'take care that the laws be faithfully executed' under Article II." *See Humphrey's Executor*, 295 U.S. at 631-32; *Free Enterprise*, 561 US at 498, 506, 516 (refusing to issue a blanket rule that dual-layer tenure protections are *per se* unconstitutional).

For example, in *Free Enterprise*, the Supreme Court evaluated the tenure protections afforded the Public Company Accounting Oversight Board, who were conceded to be Inferior Officers under the oversight of the independent Security Exchange Commission (SEC). 561 U.S. at 486-87 (noting that SEC Commissioners, as an independent agency, could only be removed by the President for cause). The Board had broad authority to make policy decisions about enforcement priorities, including the authority to initiate formal investigations and disciplinary proceedings, as well as to issue severe sanctions. *Id.* at 484-85, 505. The Court found that the Board could act with "significant independen[ce]" in determining its priorities and actions without SEC preapproval or direction, and that its tenure protections "substantially insulated" it from the SEC's control. *Id.* at 486, 505. The Court found that the Board's tenure protections, in combination with the tenure protections afforded SEC Commissioners, impermissibly "impaired" the ability of the President to remove Board members if unhappy with their performance. *Id.* at 496-97 ("By granting the Board executive power without the Executive's oversight, this Act subverts the President's ability to ensure that the laws are faithfully executed – as well as the public's ability to pass judgment on his efforts."). Given the Board's role in "determin[ing] the policy and enforce[ing] the laws of the United States," the Court held that the Board's tenure protections violated the separation of powers and were unconstitutional. *Id.* at 483-84, 505.

Here, unlike the Board in *Free Enterprise*, the ALJ's functions are limited in scope, fall outside core executive authority, and are subject to the plenary review of the Commission. For example, FTC ALJs do not determine enforcement priorities: they do not have the authority to initiate enforcement proceedings, and they cannot issue final orders finding or remedying FTC Act violations. Instead, the Commission alone decides whether to issue a complaint, accept a

settlement agreement and issue a consent order, issue a final decision as to whether a respondent has violated the FTC Act, and to impose any appropriate remedies. *See*, *supra*, Argument, § I.A.1.1 (FTC ALJs Are Not Inferior Officers), at 51. Finally, unlike the Board in *Free Enterprise* that was "substantially insulated from the Commission's control," FTC ALJ actions are subject to the plenary review of the Commission. *See id.*; *see also Free Enterprise*, 561 U.S. at 486. Indeed, the *Free Enterprise* Court specifically noted that ALJs are not similarly situated to the Board, and explicitly excluded them from the scope of its ruling. *Free Enterprise*, 561 U.S. at 507, n.10 (reasoning that many ALJs perform "adjudicative rather than enforcement or policymaking functions," or "possess purely recommendatory powers"); *see also Duka v. SEC*, No. 15 Civ. 357(RMB)(SN), 2015 WL 1943245, at *8-10 (S.D.N.Y. Apr. 15, 2015) (rejecting similar dual tenure challenge to SEC ALJs because "Congressional restrictions upon the President's ability to remove 'quasi judicial' agency adjudicators are unlikely to interfere with the President's ability to perform his executive duties"); Elena Kagan, *Presidential Administration*, 114 Harv. L. Rev. 2245, 2363 (2001) (noting that presidential involvement in agency adjudications "would contravene procedural norms and inject an inappropriate influence into the resolution of controversies").

Thus, even assuming that FTC ALJs are Inferior Officers, which they are not, the ALJ's tenure protections do not violate the separation of powers, and this Court should deny the Respondent's Sixth Affirmative Defense.

d. Respondent's Sixth Affirmative Defense Should Be Denied Even Assuming *Arguendo* That There is an Appointments Clause Violation.

Finally, even assuming *arguendo* that there has been an Appointments Clause violation, which there has not, such a violation only attacks the manner of the evidentiary hearing and does

not limit or preclude Respondent's liability under the FTC Act. Thus, even if an Appointments Clause violation were found, it does not warrant the dismissal of the Complaint. Instead, this Court should certify the question of the appropriate remedy to the Commission. 16 C.F.R. § 3.23(b).

For example, the Commission's *de novo* review of the Initial Decision may cure any potential Appointments Clause violation. *See Ryder v. U.S.*, 515 U.S. 177, 187-88 (1995) (finding Court of Military Appeals' subsequent review of decision by an improperly appointed Coast Guard Court of Military Review would not cure an Appointments Clause violation in part because such review did not apply a *de novo* review standard). Alternatively, the Commission may decide to cure an alleged Appointments Clause violation by re-litigating the same complaint against Respondent by appointing one or more Commissioners to preside over the administrative hearing. *See id.* (remanding case for new hearing before properly appointed court panel after finding Appointments Clause violation); *Hill v. SEC*, No. 1:15-CV-1801 LMM, 2015 WL 4307088, at *19 (N.D. Ga. June 8, 2015) (acknowledging alleged Appointments Clause violation relating to an upcoming hearing before an SEC ALJ could be "easily cured" by the SEC pursuing the same claim in federal court or in an administrative hearing before an SEC Commissioner); 16 CFR § 3.42 (Commission has discretion to determine whether the Commission, one or more Commissioners, or an ALJ will preside over matter).

Respondent's Appointments Clause defense is without merit and should be rejected. However, even if this Court were to find an Appointments Clause violation, this Court should not dismiss this action but instead certify the question of the appropriate remedy to the Commission.

B. HIPAA Does Not Preempt Section 5

LabMD rehashes various arguments as to why HIPAA preempts the FTC Act, all of which the Commission has rejected in its previous Orders. First, LabMD suggests that the FTC Act is a general grant of authority that cannot trump the specific provisions of HIPAA. The Commission previously rejected this argument because HIPAA and the FTC Act do not conflict and are, in fact, "largely consistent." Comm'n Order Denying Resp't's Mot. to Dismiss at 11 (Jan. 16, 2014). The Commission went on to state:

> nothing in the FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa. It is not unusual for a party's conduct to be governed by more than one statute at the same time, as "'we live in an age of overlapping and concurrent regulatory jurisdiction.'" LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other.

Id. at 12-13 (citations omitted).[25]

Second, LabMD appears to argue that the FTC's Health Breach Notification Rule has some relevance to this proceeding, quoting extensively from the Commission's statement of basis and purpose accompanying the Rule. Resp't's Post-Trial Brief at 48-50. The FTC's Health Breach Notification Rule addresses the circumstances under which certain entities must

---

[25] LabMD cites to *FDA v. Brown & Williamson*, 529 U.S. 120 (2000) and other cases where there was an actual conflict between two provisions, and the specific one was held to "trump" the general one. The Commission has already distinguished *Brown & Williamson* and another case similar case cited by LabMD – *Credit Suisse Securities, LLC v. Billing*, 551 U.S. 264 (2007) – on the grounds that the two provisions in those cases conflicted, unlike in the present case, where HIPAA and the FTC Act do not. Comm'n Order Denying Resp't's Mot. to Dismiss at 12-13 (Jan. 16, 2014). The Third Circuit has also rejected a challenge based on *Brown & Williamson* to the Commission's power to bring Section 5 cases in the data security area. *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *7-*8 (3d Cir. Aug. 24, 2015).

notify consumers of a security breach. *See* 16 C.F.R. Part 318. It does not contain any independent data security requirements. As the Commission pointed out in its Order on LabMD's Motion to Dismiss, this Rule is irrelevant in this proceeding, because "the Complaint in the present proceeding alleges only statutory violations; it does not allege violations of the FTC's Health Breach Notification Rule." Comm'n Order Denying Resp't's Mot. to Dismiss at 12 n.20 (Jan. 16, 2014). To the extent LabMD is arguing that, because the Rule does not apply to HIPAA covered entities, Section 5 should not apply to HIPAA covered entities, the Commission rejected this argument in its Order Denying LabMD's Motion to Dismiss. *Id.*[26]

Finally, LabMD appears to argue that the evidence in this case – introduced after the Commission's Order Denying LabMD's Motion to Dismiss – shows that HHS "permitted" LabMD's activities, and that therefore there is a "clear repugnancy" between HHS's standards and the Commission's actions. Resp't's Post-Trial Brief at 50. LabMD pointed to *no* evidence that HHS "permitted" LabMD's activities or that LabMD otherwise complied with HIPAA, in violation of the Court's Order on Post-Trial Briefs. In fact, LabMD affirmatively declined to provide evidence on its HIPAA compliance. CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Response to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence"). As the Commission noted in its Order Denying LabMD's Motion for Summary Decision, "LabMD points to no record evidence regarding what measures, if any, it implemented to prevent data breaches. It does not explain which HIPAA

[26] It is equally unclear why LabMD cites to former Commissioner Wright's statement about unfair *competition. See* Resp't's Post-Trial Brief at 48-50. The statement of one Commissioner on a wholly unrelated subject is irrelevant to the applicable law or facts of this case.

standards apply to LabMD's actions or why LabMD's conduct satisfied them. Indeed, LabMD does not even assert that it *complied* with the applicable HIPAA Standards." Comm'n Order Denying Resp't's Mot. for Summary Decision at 5 (May 19, 2014). Respondent points to no evidence that has changed that analysis since the order was issued. The Order further notes that, even if LabMD could show evidence that it complied with HIPAA, "[we] held in the Order denying LabMD's Motion to Dismiss that HIPAA does not 'trump' Section 5, and that LabMD therefore 'cannot plausibly assert that, because it complies with [HIPAA], it is free to violate' requirements imposed independently by Section 5 of the FTC Act." *Id.* (citations omitted). LabMD's attempt to re-argue an issue that the Commission has ruled upon multiple times must fail.

C. LabMD's Due Process Rights Have Not Been Violated in this Proceeding

1. LabMD Had Fair Notice of What Conduct is Unfair

a. Section 5 Provides Fair Notice of What Conduct is Unfair[27]

The Commission is not required to promulgate rules relating to data security before enforcing Section 5 in the data security context. Comm'n Order Denying Resp't's Mot. to Dismiss at 14-15 (Jan. 16, 2014) ("[A]dministrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue"); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 619 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (finding that precedent does not "require[] the FTC to formally publish a regulation before

[27] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

bringing an enforcement action under Section 5's unfairness prong"). Instead, it can choose to proceed by adjudication, as it has done here. *See POM Wonderful, LLC v. FTC*, 777 F.3d 478, 497 (D.C. Cir. 2015) (affirming that the Commission "validly proceeded by adjudication" and is not required to engage in rulemaking even where an administration decision may "affect agency policy and have general prospective application" (citations omitted)); *SEC v. Chenery Corp.*, 332 U.S. 194, 202-03 (1947) (holding that agencies "must be equipped to act either by general rule or *by individual order*" and "retain power to deal with [] problems on a case-to-case basis if the administrative process is to be effective" (emphasis added)).[28]

[28] The two cases upon which LabMD relies in its Post-Trial Brief are distinguishable. *FCC v. Fox Television Stations, Inc*. concerned the retroactive application of a changed agency policy. *F.C.C. v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2318 (2012) ("[The FCC's] lack of notice to Fox and ABC that *its interpretation had changed* so the fleeting moments of indecency contained in their broadcasts were a violation . . . 'fail[ed] to provide a person of ordinary intelligence fair notice of what is prohibited.'" (emphasis added) (citation omitted). Here, the Commission "has repeatedly affirmed its authority to take action against unreasonable data security measures as 'unfair . . . acts or practices' in violation of Section 5 . . . [and] has also confirmed this view by bringing administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal information collected from consumers online." Comm'n Order Denying Resp't's Mot. to Dismiss at 8 (Jan. 16, 2014).

LabMD's reliance upon *Satellite Broad. Co. v. FCC*, 824 F.2d 1 (D.C. Cir. 1987) is also misplaced, as the appellant in *Satellite* was penalized for violating a rule promulgated by the agency at issue, in contrast to the injunctive relief simply mandating compliance with a long-standing statute at issue in this case. *Id.* at 3-4 (stating that the dismissal of an application "is a sufficiently grave sanction to trigger this duty to provide clear notice" (citation omitted)). Here, "the complaint does not even seek to impose damages, let alone retrospective penalties." Comm'n Order Denying Resp't's Mot. to Dismiss at 17 (Jan. 16, 2014). Neither of these cases lends support to LabMD's contention that dismissal of this case would be appropriate, even if there had been inadequate notice, and LabMD provides no other support for that contention.

The unfairness definition in the FTC Act, 15 U.S.C. § 45(n), "is sufficient to give fair notice of what conduct is prohibited."[29] Comm'n Order Denying Resp't's Mot. to Dismiss at 16 (Jan. 16, 2014);[30] *see also FTC v. Wyndham Worldwide Corp.*, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 619 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (rejecting the contention that regulations are the only means to provide fair notice and stating that "Section 5 codifies a three-part test that proscribes whether an act is 'unfair'"); *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *13 (3d Cir. Aug. 24, 2015) (finding that the unfairness "standard informs parties that the relevant inquiry here is a cost-benefit analysis"). In addition to the unfairness definition in Section 5, the Commission has issued "many public complaints and consent agreements" that "'constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*.'" *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (quoting *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis added by court)); *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *15 (3d Cir. Aug. 24, 2015) (noting that courts "regularly

---

[29] This objective reasonableness test applies across industries, and operators in the medical industry that hold Personal Information are not subject to a different standard. *See infra* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

[30] The Commission has twice rejected LabMD's argument that the Commission has not provided adequate notice of what conduct is unfair. Comm'n Order Denying Resp't's Mot. for Summary Decision at 9 (May 19, 2014) ("We have already carefully addressed and disposed of LabMD's arguments that [] its due process rights were infringed and that it lacked adequate notice of what conduct is prohibited.").

consider materials that are neither regulations nor 'adjudications on the merits'" in reviewing fair notice claims).[31]

Objective tests of reasonableness are common in the law, and do not violate fair notice requirements. *See, e.g., Brooks v. Vill. of Ridgefield Park*, 185 F.3d 130, 137 (3d Cir. 1999) (employer must act as a "reasonably prudent man" would have acted to satisfy Fair Labor Standards Act (quoting *Addison v. Huron Stevedoring Corp.*, 204 F.2d 88, 92 (2d Cir. 1953)); *Brock v. Teamsters Local Union No. 863*, 113 F.R.D. 32, 34 (D.N.J. 1986) (reasonableness is determined under a "prudent man" standard, an objective standard which requires that each situation be "tried on the individual facts of th[e] case, and in light of the standard as developed in the case law"); *Romala Stone, Inc. v. Home Depot U.S.A., Inc.*, 2007 WL 6381488, at *27-28 (N.D. Ga. Apr. 2, 2007), *partially adopted by* 2007 WL 2904110 (N.D. Ga. Oct. 1, 2007) (collecting examples of "reasonable man"-type standards from patent, trademark, criminal, judicial recusal, and contract jurisprudence).

Indeed, negligence law already imposes the same standard of care, including for data security practices. *See In re Zappos.com, Inc.*, 2013 WL 4830497, at *3-4 (D. Nev. Sept. 9, 2013) (applying "reasonable and prudent person" standard in negligence case for failure to safeguard electronically held data). The Section 5(n) factors parallel the basic considerations that inform tort liability under the same circumstances.

---

[31] Mr. Kaufman's testimony was neither intended to, nor did it purport to, address "due process standards." Instead, Mr. Kaufman simply identified materials that provide guidance; the standards the Commission uses to determine whether an entity's data security practices are unfair under Section 5 was not a permissible topic of examination under the Court's March 10, 2014 order. *See* Order Granting in Part and Denying in Part Compl. Counsel's Mot. for Prot. Order Re Rule 3.33 Depo. at 6-7 (Mar. 10, 2014) ; *see also* RX 532 (Kaufman, Dep. at 7-8). Accordingly, it is disingenuous for LabMD to characterize Mr. Kaufman's testimony as having addressed "due process standards."

Duties to act "reasonably" and to follow similarly general standards of conduct are ubiquitous in statutory law as well. This general standard is applied across a wide range of industries. For example, restraints of trade under the Sherman Act are often assessed under a fact-specific "rule of reason," *see Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 899 (2007), yet violations are subject to automatic treble damages. *See* 15 U.S.C. § 15(a). Likewise, the FCC polices the obligation of common carriers to offer "just and reasonable" rates and terms of service. 47 U.S.C. § 201(b). In both of those contexts, companies can be subject to sanctions under guideposts no more specific than Section 5.

Furthermore, "[w]hen Congress created the Federal Trade Commission in 1914 and charted its power and responsibility…, it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' … by enumerating the particular practices to which it was intended to apply." *FTC v. Sperry & Hutchinson Co.*,405 U.S. 233, 239-40 (1972) (citing S. Rep. No. 63-597 at 13 (1914)).[32] Thus, instead of "attempt[ing] to define the many and variable unfair practices which prevail in commerce and to forbid their continuance," Congress adopted "a general declaration condemning unfair practices" and "le[ft] it to the commission to determine what practices were unfair." S. Rep. No. 63-597 at 13 (1914). "[T]here were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others." *Id.* As the House Conference Report put it,

---

[32] As initially enacted in 1914, Section 5 of the FTC Act prohibited only "unfair methods of competition." 38 Stat. 717, 719 (1914). In 1938, Congress broadened Section 5 to also cover "unfair or deceptive acts or practices in commerce." 52 Stat. 111 (1938). The 1938 amendment is now the main source of the FTC's consumer protection authority (as distinct from its antitrust authority). Congress' intent "was affirmatively to grant the Commission authority to protect consumers as well as competitors." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). The term "unfair" thus means the same in the 1938 amendments as in the original 1914 enactment. *See Sperry*, 405 U.S. at 244.

"[i]t is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985) (quoting H.R. Rep. No. 63-1142 at 19 (1914) (Conf. Rep.)). In short, Congress "expressly declined to delineate" the "particular acts or practices" deemed unfair, *Am. Fin. Servs.*, 767 F.2d at 969, preferring instead to give the FTC "broad discretionary authority … to define unfair practices on a flexible and incremental basis," *id.* at 967. As a result, courts have "adopted a malleable view of the Commission's authority" to interpret and apply the term "unfair." *Id.* at 967-68. "The takeaway is that Congress designed the term as a 'flexible concept with evolving content' and 'intentionally left [its] development . . . to the Commission.'" *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *3 (3d Cir. Aug. 24, 2015) (citations omitted).

"As the Supreme Court has recognized, '[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case judicial decision in the common-law tradition.'" Comm'n Order Denying Resp't's Mot. to Dismiss at 16-17 (Jan. 16, 2014) (quoting *Northwest Airlines, Inc. v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981)). Congress "intentionally left development of the term 'unfair' to the Commission rather than attempting to define" specific practices. *Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) (quoting S. Rep. No. 63-597 at 13 (1914)). Congress had a "crystal clear" intent that the term should have "sweep and flexibility," *Sperry*, 405 U.S. at 241, and should remain "a flexible concept with evolving content," *FTC v. Bunte Bros., Inc.*, 312 U.S. 349, 353 (1941); *accord In re Smith*, 866 F.2d 576, 581 (3d Cir. 1989) ("[s]tatutes prohibiting

unfair trade practices and acts have routinely been interpreted to be flexible and adaptable to respond to human inventiveness").

b. **Mr. Kaufman's Testimony Did Not Violate the APA**

The Commission is not required to, and has not, issued a "statement[] of general policy" regarding data security under the Administrative Procedures Act ("APA"), 5 U.S.C. § 552(a)(1)(D). *See* CCRRCL ¶¶ 21-22. The APA contemplates "a statement by an administrative agency announcing motivating factors the agency will consider, or tentative goals toward which it will aim, in determining the resolution of a Substantive question of regulation." *Brown Exp., Inc. v. United States*, 607 F.2d 695, 701 (5th Cir. 1979). It is "a formal method by which an agency can express its views." *Pac. Gas & Elec. Co. v. Fed. Power Comm'n*, 506 F.2d 33, 38 (D.C. Cir. 1974). Courts look to an "agency's own characterization" to "provide[] some indication of the nature of the announcement" and determine if it is a statement of general policy. *Id.*, 506 F.2d at 39.

The Commission has not issued a statement of general policy as that term is used in the APA. Respondent's argument that Mr. Kaufman's unremarkable statement that the Bureau of Consumer Protection has "published a great deal of materials that provide guidance . . . from the 50 or so settlement orders that have been issued by the FTC that provide such information to business educational [sic], to speeches, to Congressional testimony, and there's additional information available from other organizations as well," RX532 (Kaufman, Dep. at 171-72), or the Commission's publication of the same, is somehow a "statement of general policy" as that term is used in the APA is unavailing. *See* Resp't's Post-Trial Brief at 51. Mr. Kaufman's deposition statement was not "a formal method" for the agency to "express its views," and the agency did not characterize it as such. *See Pac. Gas & Elec. Co.*, 506 F.2d at 38-39.

Moreover, it is well accepted that public complaints and consent agreements "'constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance,'" *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (quoting *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis removed)), and the Commission has voted to issue more than 20 complaints charging deficient data security as unfair practices.

2. LabMD's Due Process Rights Under the Fourth Amendment Have Not Been Violated in this Proceeding

a. The Exclusionary Rule is Inapplicable[33]

Actions of a private party cannot violate the Fourth Amendment, even if the private party later gives evidence it obtained to the government. *See, e.g.*, *U.S. v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990) ("[W]here a private person delivers the fruits of his private search to police, that evidence is not excludable at trial on the basis that it was procured without a search warrant."); *U.S. v. Jacobsen*, 466 U.S. 109, 113-14 (1984) (Fourth Amendment is "wholly inapplicable" to searches by private parties); *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921).

The legal authority to which Respondent cites in support of its contention that Tiversa is somehow an agent of the Commission is inapposite. Specifically, the Supreme Court's holding in *Blum* provided that the government "can be held responsible for a private decision *only* when it has exercised *coercive power* or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State." *Blum v. Yaretsky*, 457 U.S. 991 (1982) (citations omitted) (emphasis added). The evidentiary record contains no evidence whatsoever of such conduct by the Commission or its staff.

To the extent that the Fourth Amendment applies in this case – which it does not – numerous courts have held in a Fourth Amendment analysis that there is no reasonable expectation of privacy in files made available for sharing on a P2P network. *See, e.g.*, *U.S. v. Norman*, 448 Fed. Appx. 895, 897 (11th Cir. 2011); *U.S. v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009); *U.S. v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). Moreover, it is law of the case that the provenance of the 1718 File is not dispositive of the Complaint's allegations:

> [E]ven if we accepted as true the claims that Tiversa retrieved the Insurance Aging File without LabMD's knowledge or consent . . . , that Tiversa improperly passed on that file to Professor Johnson or others . . . , and that Tiversa touted its unique technology . . . , these facts would not resolve the ultimate questions we must decide in this case. In particular, they would not compel us, as a matter of law, to dismiss the allegations in the Complaint that LabMD failed to implement reasonable and appropriate data security and that such failure caused, or was likely to cause, unavoidable and unjustified harm to consumers. To the contrary, LabMD's factual contentions concerning Tiversa and the Sacramento Police Department are fully consistent with the Complaint's allegations that LabMD failed to implement reasonable and appropriate data security procedures.

Comm'n Order Denying Resp't's Mot. for Summary Decision at 6-7 (May 19, 2014).

"Misconduct by other actors is a proper target of the exclusionary rule only insofar as those others are 'adjuncts to the law enforcement team.'" *U.S. v. Herring*, 492 F.3d 1212, 1217 (11th Cir. 2007) (quoting *Arizona v. Evans*, 514 U.S. 1, 15 (1995)). The Fourth Amendment protects an expectation of privacy against unreasonable government intrusion, not "the mere expectation . . . that certain facts will not come to the attention of the authorities." *Jacobsen*, 466 U.S. at 122. In this instance, the time lapse of over a year between when Tiversa first contacted

---

[33] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

LabMD and provided it with the 1718 File and when the FTC sought the file through process indicates that Tiversa was not acting at the direction of or in conjunction with the Commission[34] when it obtained the file.[35] This falls squarely within the Supreme Court's holding in *Jacobsen* and *Burdeau*.

If Tiversa obtained the 1718 File in violation of the law[36] – a question that need not be resolved – the Fourth Amendment does not mandate that the evidence be excluded in the FTC's proceeding against LabMD. *See Clutter*, 914 F.2d at 778 ("[T]he exclusionary rule of the Fourth Amendment does not apply to a search and seizure by a private person not acting in collusion

---

[34] In February 2008, Mr. Wallace downloaded the 1718 File from a P2P network. Wallace, Tr. 1393-95. In May 2008, LabMD was informed that the 1718 File was available on a P2P network and provided with a copy of the 1718 File downloaded from the P2P network. CCFF ¶ 1395. The 1718 File was provided to the Commission more than a year later, in 2009. Wallace, Tr. 1352-1353,1361-1362, 1365, 1452.

[35] Professor Johnson also confirmed that the FTC did not participate in his research involving the 1718 File. CX0721 (Johnson Dep.) at 95.

[36] Respondent's contention that Tiversa's actions with respect to the 1718 File violated state or federal law is not supported by the evidentiary record or applicable law. 18 U.S.C. § 1030 is the federal Computer Fraud and Abuse Act ("CFAA"). The CFAA, like the Georgia CSPA, is a criminal statute that permits civil suits for violations. It, too, prohibits accessing a computer "without authorization." 18 U.S.C. § 1030(a)(2), (4). Courts have consistently held that accessing publicly available information, including a P2P sharing folder, is not "without authorization." *See, e.g., Motown Record Co. L.P. v. Kovalcik*, 2009 WL 455137, at *3 (E.D. Pa. Feb. 23, 2009) ("The fact that the accessed files were in the [P2P] share folder negates the second element under the statute that Plaintiffs acted without authorization or exceeded the authorization given to them. No authorization was needed since the files accessed were accessible to the general public." (emphasis added)); *Loud Records LLC v. Minervini*, 621 F. Supp. 2d 672, 678 (W.D. Wisc. 2009) (finding that "because the [P2P] files that plaintiffs allegedly accessed were accessible by the public, any allegation . . . that plaintiffs acted without authorization is tenuous at best"); *see also Cvent v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 933 (E.D. Va. 2010) (no violation of CFAA where a competitor copied content from a website to which "the entire world was given unimpeded access"). *See* CCRRCL ¶¶ 121-125.

with law enforcement officials . . . ."). This is in accord with Eleventh Circuit's observation in *Herring* that the purpose of the exclusionary rule is deterrence of government misconduct. *Herring*, 492 F.3d at 1216 (citing *U.S. v. Janis*, 428 U.S. 433 (1976)). Where the government did not participate in the seizure of the evidence, exclusion does not accomplish a deterrent purpose.

b. **LabMD's Due Process Rights Are Amply Protected**

At every stage in this proceeding – from the Commission's approval of the Complaint through Complaint Counsel's disclosures to the parties and the Court – the Commission, Complaint Counsel, and this Court have protected Respondent's due process rights. LabMD's assertion to the contrary – which is predicated on Respondent's suggestion that Complaint Counsel's alleged failure to discharge a supposed duty to investigate a third-party witness somehow taints the entire proceeding – is fundamentally flawed because Commission investigations are not predicated on the establishment of probable cause or even reasonable suspicion that a violation has occurred. *See FTC v. Carter*, 636 F.2d 781, 786 (D.C. Cir. 1980) (the FTC "can investigate merely on suspicion that the law is being violated, *or even just because it wants assurance that it is not*. . . . [T]he Commission is not limited by forecasts of probable result of the investigation." (emphasis added) (internal quotation marks and citation omitted)).

Without any citation to the evidentiary record, Respondent baldly asserts that "FTC knew Boback lied no later than May 30, 2014." Resp't's Post-Trial Br. at 55. Respondent's contention in this regard is false and provides no basis for finding any violation of due process.[37]

[37] During an *in camera* session initiated at the request of Respondent's counsel, [redacted]

Respondent's further contention that "Complaint Counsel knew or should have known that the long-held information contained in exhibit CX0307 was diametrically opposed to the information contained in CX0019," Resp't's Post-Trial Br. at 55, is similarly without foundation. Indeed, Complaint Counsel asked Mr. Boback a number of questions about the IP address that appears on CX0307:

> Q. There is an IP address on the right-hand side, it is 64.190.82.42. What is that?
> A. That, if I recall, is an IP address that resolves to Atlanta, Georgia.
> Q. Is that the initial disclosure source?
> A. We believe that it is the initial disclosure source, yes.
> Q. And what is that based on?
> A. The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.
> Q. Would that not be true if you found the file on a third site?
> A. If they had the same file as well, the same hash, that would also show another IP address, which could potentially be the initial disclosure source. However, this was the only disclosure source that

---

[redacted]

> we found at that time when we looked at it for our other client to identify the initial disclosure source.

CX0703 (Boback, Tiversa Designee, Dep. at 97-164). Mr. Boback's explanation – that one exhibit reflected "an initial disclosure source," while the other reflected a "download" location – was unremarkable, and did not need further inquiry. In any event, during Respondent's examination, Respondent did not ask Mr. Boback a single question regarding CX0307, which Complaint Counsel produced with its Initial Disclosures nearly two months before the November 21, 2013 deposition. Respondent cannot now claim that its own counsel's failure to have examined Mr. Boback about any purported discrepancy constituted a due process violation necessitating the suppression of evidence or the dismissal of this action.

Similarly, after opposing Complaint Counsel's effort to take discovery of Tiversa and its employees [redacted], Respondent cannot now level constitutional criticisms at Complaint Counsel for having failed to adduce sufficient evidence of how, when, and where Tiversa found the 1718 File on the P2P networks.

3. LabMD's Privileges Were Respected at Mr. Kaloustian's Investigational Hearing

Complaint Counsel complied fully with all applicable rules of professional responsibility and the Commission's Rules of Practice governing investigational hearings when it conducted an investigational hearing of Curt Kaloustian, a former employee of LabMD, on May 3, 2013.[39]

---

[38] [redacted]

[39] At the time of Mr. Kaloustian's investigational hearing, the Commission had not issued its complaint. Accordingly, Commission counsel were not acting as "Complaint Counsel." For the

Therefore, the exclusionary rule does not prevent Complaint Counsel and its experts from relying on evidence obtained during Mr. Kaloustian's investigational hearing.

Neither Commission Rules nor the D.C. Rules of Professional Conduct require Complaint Counsel to seek LabMD's consent before deposing its former employees. *See* Commission Rules of Practice § 2.7(f)(3) and § 2.9, 16 C.F.R. §§ 2.7, 2.9; *see also* D.C. Rule of Professional Conduct 4.2, Comment 6; D.C. Bar Legal Ethics Comm. Op. 287 (1998); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 91–359 (1991); *Domestic Air Transportation Antitrust Litig.*, 141 F.R.D. 556, 561-62 (N.D. Ga. 1992); *U.S. v. Western Elec. Co.*, No. 82-1092, 1990 WL 39129, at *2 (D.D.C. Feb. 28, 1990).[40] As Mr. Kaloustian is a former employee with no continuing relationship with LabMD, it was proper for Complaint Counsel to contact him without LabMD's consent.

Indeed, the D.C. Rules of Professional Conduct permit ex parte contact between Complaint Counsel and a former employee of LabMD, subject to observance of certain safeguards. Complaint Counsel fully observed these safeguards and scrupulously avoided intruding on LabMD's attorney-client privilege, attorney work product or trade secret protections, or possible confidentiality agreement during the investigational hearing. *See* D.C.

---

ease of the reader, this discussion uses "Complaint Counsel" throughout, even though Commission counsel were acting in a different capacity.

[40] Respondent's reliance on case law interpreting Maryland State Bar Rules is unfounded, as neither Complaint Counsel who participated in Mr. Kaloustian's investigational hearing is a member of the Maryland bar and the Maryland district court's interpretation of Rule 4.2, *Camden v. State of Maryland*, 910 F. Supp. 1115 (D. Md. 1996), is a minority position. Resp't's Post-Trial Brief at 57. The majority of courts that have considered the issue have concluded former employees are not included in the rule prohibiting *ex parte* communications, and counsel may contact former employees so long as they do not discuss privileged information. *See* D.C. Bar Legal Ethics Comm. Op. 287 (1998) (collecting cases).

Rule 4.2 Comment 6 (requiring Complaint Counsel not "seek to obtain information that is otherwise protected"); D.C. Rule of Professional Conduct 4.4(a) and Comment 1 (advising counsel not to engage in "unwarranted intrusions into privileged relationships, such as the client-lawyer relationship"). Consistent with their professional obligations, Complaint Counsel specifically instructed Mr. Kaloustian not to reveal any information protected by LabMD's attorney-client privilege, work product or trade secret protections, or confidentiality agreement. CX0735 (Kaloustian, IHT at 8-10). During the deposition, Complaint Counsel instructed Mr. Kaloustian not to testify about the Tiversa LimeWire investigation and reminded Mr. Kaloustian, when appropriate, not to reveal privileged information. CX0735 (Kaloustian, IHT at 74, 76, 88, 220, 259, 264, 269-271).

Significantly, when LabMD counsel was present at the deposition of another former employee who had previously been examined in an *ex parte* investigational hearing, counsel did not take any opportunity to assert privilege over the former employee's current or previous testimony. Complaint Counsel conducted an investigational hearing and a deposition of Alison Simmons, a former IT employee and a contemporary of Mr. Kaloustian's at LabMD, and covered many of the same topics as were covered in the investigational hearing of Mr. Kaloustian. *See* CX0734 (Simmons, IHT, May 2, 2013); CX0730 (Simmons, Dep., Feb. 5, 2014); CCFF ¶ 371 (Simmons worked at LabMD from October 2006 through August 2009), 349 (Kaloustian worked at LabMD from October 2006 through April or May 2009). At the investigational hearing, Complaint Counsel provided special instructions to Ms. Simmons regarding LabMD's attorney client privilege, work product and trade secret protections, and confidentiality agreement. CX0734 (Simmons, IHT at 9-13). Complaint Counsel followed a clear procedure throughout the investigational hearing to ensure that there was no inadvertent

disclosure of privileged information. CX0734 (Simmons, IHT at 42, 43, 67, 148, 157, 160, 161-62). At the subsequent deposition, LabMD was present and represented by counsel. CX0730 (Simmons, Dep., Feb. 5, 2014). Although Respondent's counsel made a number of objections on the record, she did not take any opportunity to assert privilege over Ms. Simmons' current or previous testimony. *See, e.g.*, CX0730 (Simmons, Dep. at 107-08).

The blanket no-contact rule advocated by LabMD is inconsistent with interpretations of D.C. Rules of Professional Conduct and would impose burdens on the Commission's ability to obtain evidence. *See* D.C. Bar Legal Ethics Comm. Op. 287 (1998). First, it contradicts the broad policy that litigants should have access to all relevant, non-privileged information regarding a matter and, derivatively, lawyers should be allowed to find facts as quickly and inexpensively as possible. *Id*. Second, it would act as a deterrent to the disclosure of information. Former employees would be reluctant to come forward with potentially damaging information if they could only do so in the presence of the company's attorney. Third, because former employees cannot bind the company by decision making, by conduct, or by admission with respect to a pending or prospective matter, Rule 4.2 does not prohibit *ex parte* contacts with these individuals. *Id*. The fact that former employees may possess information prejudicial to their former employer does not, without more, place those former employees in a position to bind the organization in the manner contemplated by Rule 4.2. *Id*. Given that Complaint Counsel put in place safeguards to prevent the inadvertent disclosure of privileged material, this Court should not exclude the uncontroverted facts obtained during the investigational hearing of Mr. Kaloustian.

Finally, even if Mr. Kaloustian's investigational hearing somehow infringed on LabMD's privileges, the factual evidence adduced in that deposition should not be excluded. LabMD has

not identified *any* alleged privileged information Mr. Kaloustian revealed. Indeed, it cites only to discrete facts it contends should be excluded. Resp't's Post-Trial Brief at 57 n.12, 76-77. Putting aside the issue of LabMD's failure to prove the elements of attorney-client privilege, it is black letter law that facts are never protected by privilege:

> "A fact is one thing and a communication concerning that fact is an entirely different thing. The client cannot be compelled to answer the question, 'What did you say or write to the attorney?' but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney."

Upjohn Co. v. U.S., 449 U.S. 383, 395-96 (1981) (quoting *Philadelphia v. Westinghouse Elec. Corp.*, 205 F. Supp. 830, 831 (E.D. Pa. 1962)).

Because Complaint Counsel's conduct during the investigational hearing was proper, the exclusionary rule does not prevent Complaint Counsel or its experts from using facts obtained from Mr. Kaloustian during the investigational hearing.

4. This Proceeding Has Not Infringed on LabMD's Right to a Fair Process

Respondent's claim that it has been denied due process based on the alleged appearance of prejudgment and bias by the Commission is both based on a misstatement of the law and is unsupported by the record.

a. The Commission's 2009 Amendments to its Rules of Practice Do Not Deny Litigants Due Process[41]

Respondent's argument that the 2009 amendments to the Commission's Rules of Practice violate due process by "blending of prosecutorial, legislative, and adjudicative functions, and wrongfully curtail[ing] this Court's authority" is flatly wrong. Resp't's Post-Trial Brief at 57. *See FTC v. Cement Inst.*, 333 U.S. 683, 702-03 (1948). The 2009 revisions to the Rules of

[41] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

Practice were designed to "expedite resolution of a matter and save litigants resources." FTC, Rules of Practice, 73 Fed. Reg. 58832-01 (proposed Oct. 7, 2008) (to be codified at 16 C.F.R. pts. 3, 4). Due process "is not a technical conception with a fixed content unrelated to time, place and circumstances," *Cafeteria & Restaurant Workers v. McElroy*, 367 U.S. 886, 895 (1961) (internal quotation omitted), but "calls for such procedural protections as the particular situation demands," *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972). In the context of administrative adjudications, courts long ago "reject [ed] the idea that the combination of judging and investigative functions is a denial of due process." *Withrow v. Larkin*, 421 U.S. 35, 52 (1975) (internal quotations and citations omitted); *see also Intercon'l Indus., Inc. v. Am. Stock Exch.*, 452 F.2d 935, 943 (5th Cir. 1971) ("The principle is well established . . . that due process is not violated when an administrative agency exercises both investigative and judicial functions."). Rather, in formal agency adjudicatory proceedings, due process is satisfied when the agency follows the requirements of the APA. *Withrow*, 421 U.S. at 51-52; *see also FTC v. Cinderella Career & Finishing Sch., Inc.*, 404 F.2d 1308, 1315 (D.C. Cir. 1968) (citing numerous sources).

The revised Rules of Practice accord plaintiff due process because they comport fully with the APA. The revised Rule 3.22(a) provides that motions to dismiss administrative complaints "shall be directly referred to and ruled on by the Commission." 16 C.F.R. § 3.22(a). Contrary to respondent's implication that this violates due process, the APA contains no requirement that the ALJ play any role at all in adjudications conducted pursuant to 5 U.S.C. §§ 554 and 556, and it certainly does not require the ALJ to address dispositive motions in the first instance. Indeed, the APA allows the *entire* adjudication to be presided over *either* by an ALJ, *or* by "the agency" *or* by "one or more members of the body which comprises the agency."

5 U.S.C. § 556(b). The APA thus clearly permits the Commission, rather than the ALJ, to rule on a motion.

Moreover, the APA authorizes "[t]he agency . . . in its sound discretion, to issue a declaratory order to . . . remove uncertainty." 5 U.S.C. § 554(e). By using the term "the agency," the statute contemplates issuance of such an order by the agency acting as a whole and says nothing about an ALJ considering such rulings in the first instance. The Commission's hearing of dispositive motions "remove[s] uncertainty." For example, the Commission's order denying LabMD's Motion to Dismiss in this case "removed uncertainty" about the scope of the FTC's authority over LabMD's data security practices and enabled this Court to narrow discovery and avoided wasteful development of irrelevant evidence.

Both the APA and the FTC Act authorize the agency to review an ALJ's factual and legal conclusions de novo. 5 U.S.C. § 557(b); 15 U.S.C. § 45(b), (c). Because the APA allows the Commission to set aside an ALJ ruling, Respondent's implication that due process is violated by allowing the Commission to rule on a dispositive motion in the first instance is without merit.

b. **This Proceeding Will Be Decided on its Merits**

Respondent's claim that it has been denied due process because it is allegedly "a statistical certainty" that the Commission will ultimately rule against it is completely unsupported by law or fact. Respondent has presented no evidence to support its claim that the Commission "will find LabMD's data security practices are unfair under Section 5(n) no matter what this Court does." Resp't's Post-Trial Brief at 58. The citation to two articles is an improper attempt to prove facts through evidence that has not been admitted and without any expert opinion on which this supposed statistical analysis is based. Respondent has presented no evidence or argument to otherwise support this claim.

In any event, not even the articles cited by Respondent support their claim that it is a "statistical certainty" that the Commission will find that LabMD violated Section 5. *See* Nicole Durkin, Essay, *Rates of Dismissal in FTC Competition Cases from 1950–2011 and Integration of Decision Functions*, 81 Geo. Wash. L. Rev. 1684 (2013) (addressing only competition cases); Joshua Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, 11(2) Competition Pol'y Int'l Antitrust Chron. 2 (Nov. 2013), *available at* https://www/competitionpolicyinternational.com/file/view/7027 (addressing only FTC's competition cases). Even related to competition cases, a recent competition case shows that Complaint Counsel does not prevail on every claim brought against a respondent. *McWane & StarPipe Prods.*, Docket No. 9351, 2014 WL 556261, at *2-3 (F.T.C. Jan. 30, 2014) (dismissing all but one of seven counts brought against respondent). Looking to the more relevant universe of consumer protection cases, given how few consumer protection cases have been brought administratively, any "statistical" conclusions about patterns in past cases are completely without merit. At the very least, Respondent's claim that Complaint Counsel is assured a total victory before the Commission oversimplifies prior Commission cases. *See, e.g.*, *POM Wonderful, LLC*, Docket No. 9344, 2013 WL 268926, at *65 (F.T.C. Jan. 16, 2013) (upholding ALJ's rejection of relief sought by Complaint Counsel).

Even if Respondent had presented any evidence that the Commission always rules against respondents before it, which it has not, it has offered no authority to support its claim that this would constitute a due process violation. Respondent has not shown that the Commission has in this case already decided the "specific factual questions and is impervious to contrary evidence." *Metro. Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1165 (D.C. Cir. 1995) (internal quotation marks and citations omitted) (holding that recusal of FCC Commissioner not

required absent such a showing). A claim about the Commission's decisions in prior cases does nothing to show that it has already made its determination in this one. This is especially true here, as this is the first administrative case brought by the Commission applying Section 5 to data security practices. The fact that the Commission has previously found that other respondents in other unrelated cases have violated Section 5 does not mean that it has already decided any important factual or legal question in this case. In order to show a denial of due process a party must show that the factfinder "has indicated his belief that named individuals or firms are violating the statute," not that the factfinder has found that other respondents in other unrelated cases have violated the law. *Dean Foods Co.*, Docket No. 8674, 70 F.T.C. 1146, 1966 WL 88197, at *107 (1966); *see also FTC v. Cement Inst.*, 333 U.S. 683, 701-02 (1948) (rejecting a claim that Commission's prior conclusions about underlying legal issues denied respondent due process in the present case). Respondent has not and cannot point to any authority or evidence on the record to support its argument.

c. **LabMD's First Amendment Rights Have Not Been Infringed**

Respondent has failed to establish that its due process rights have been violated, and its allegation that the Commission initiated this action in retaliation for Respondent's exercise of its First Amendment rights fails. Resp't's Post-Trial Brief at 59-60. Respondent has introduced no evidence of any animus by any individual at the Commission, nor of any causal nexus between any animus and the alleged retaliation, much less sufficient evidence to overcome the presumption that agency officials "'have properly discharged their official duties.'" *U.S. v. Armstrong*, 517 U.S. 456, 463 (1996) (quoting *United States v. Chemical Found.*, 272 U.S. 1, 14-15 (1926)). Rather, Respondent's argument appears to rely solely on the timing of the FTC

enforcement action and Mr. Daugherty's public criticism of the FTC in his published book and in other public statements.

Here, Mr. Daugherty's book was published three years after the FTC began investigating LabMD. A causal connection cannot plausibly be inferred from timing when the alleged protected speech occurs in the middle of an ongoing action. *See Slattery v. Swiss Reinsurance Am. Corp.*, 248 F.3d 87, 95 (2d Cir. 2001) ("[Where] gradual adverse job actions began well before the plaintiff had ever engaged in any protected [first amendment] activity, an inference of retaliation does not arise."); *see also Lauren W. ex rel. Jean v. DeFlaminis*, 480 F.3d 259, 267 (3d Cir. 2007) (declining to infer retaliation unless the timing is "unusually suggestive); *Swanson v. Gen. Servs. Admin.*, 110 F.3d 1180, 1188 (5th Cir. 1997) (timing must be close to support inference of retaliation). Respondent's unsupported retaliation claims should therefore be denied.

d. The Commission's Response to OGR's Request For Information Does Not Demonstrate Bias

The impartiality of an adjudicative tribunal is called into question "only if the congressional communications posed a serious likelihood of affecting the agency decision maker's ability to act fairly and impartially in the matter before it." Comm'n Op. and Order Denying Resp't LabMD, Inc.'s Mot. to Disqualify Chairwoman Edith Ramirez at 2 (June 15, 2015) ("Comm'n Order on Mot. to Disqualify"). Courts examine "not the mere fact of the inquiry, but whether there is a direct connection between the congressional involvement and the adjudicator's decision-making process." *Id.* at 2 (citing *ATX, Inc. v. U.S. Dep't of Transp.*, 41 F.3d 1522, 1527 (D.C. Cir. 1994); *Aera Energy LLC v. Salazar*, 642 F.3d 212, 220 (D.C. Cir. 2011)); *see also* Comm'n Op. and Order Denying Resp't LabMD, Inc.'s Amend. Second Mot. to Disqualify Chairwoman Edith Ramirez at 2 (Aug. 14, 2015) ("Comm'n Order on Second Mot. to

Disqualify") ("[T]he Oversight Committee's correspondence did not focus upon—or even address—Chairwoman Ramirez's decisionmaking process on the merits of the adjudication.").

The inquiries from a member of Congress in this matter related to an evidentiary source. Comm'n Order on Mot. to Disqualify at 2. They did not focus "directly and substantially upon the mental decisional processes of a Commission." *Pillsbury Co. v. FTC*, 354 F.2d 952, 954 (5th Cir. 1966). Only in that circumstance may an agency's interaction with Congress intrude on "the right of private litigants to a fair trial and . . . to the appearance of impartiality." *Pillsbury*, 354 F.2d at 964; *see also California ex rel. State Water Res. Control Bd. v. FERC*, 966 F.2d 1541, 1552 (9th Cir. 1992) (no violation of *ex parte* communications provision of APA where agency engaged in correspondence with Congress on issues related to a proceeding where there was no showing that "any such communication unduly influenced the merits of the FERC decision"). As the Commission observed, in this circumstance "no evidence shows that the Chairwoman took part in addressing the questions raised by the Oversight Committee or that she engaged in *ex parte* communications regarding the merits of this case." Comm'n Order on Second Mot. to Disqualify at 2.

The mere existence of a congressional investigation is not enough to demonstrate prejudgment. Comm'n Order on Mot. to Disqualify at 2-3. Such an absurd result would upend the adjudicative process. *See* Comm'n Order on Mot. to Disqualify at 2-3 ("[N]o agency adjudication could ever proceed if there were any congressional involvement . . . .").

B. The Commission Has Not Violated the Rule-Making Provisions of the APA[42]

1. The Commission Validly Proceeded by Adjudication in this Matter[43]

[42] Complaint Counsel responded to Respondent's arguments relating to alleged *ex parte* communication, Resp't's Post-Trial Brief at 63-64, *supra.* Argument, § 1.C.4.d (The Commission's Response to OGR's Request for Information Does Not Demonstrate Bias).

The Commission is not enforcing any "statements of general policy" on data security, as that term is used in the APA, because it has not issued any. A "statement[] of general policy" under the APA, 5 U.S.C. § 552(a)(1)(D), is "a statement by an administrative agency announcing motivating factors the agency will consider, or tentative goals toward which it will aim, in determining the resolution of a Substantive question of regulation." *Brown Express, Inc. v. United States*, 607 F.2d 695, 701 (5th Cir. 1979). It is "a formal method by which an agency can express its views." *Pac. Gas & Elec. Co. v. Fed. Power Comm'n*, 506 F.2d 33, 38 (D.C. Cir. 1974). While the Commission has provided guidance to businesses on complying with Section 5, as illustrated by the publications cited by Respondent in RCL ¶ 33[44] and its prior consent agreements[45] relating to data security, the Commission has not issued any rules or statements of general policy on data security standards. Courts look to an "agency's own characterization" to "provide[] some indication of the nature of the announcement" and determine if it is a statement of general policy. *Pac. Gas & Elec. Co.*, 506 F.2d at 39. The Commission has not so designated any of the guidance it has provided.

---

[43] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

[44] The term "guide" does not appear in 15 U.S.C. § 57a(a)(1), which permits the Commission to issue interpretive rules and general statements of policy. The Commission does produce guides and guidance for business, but such guides are not interpretive rules or general statements of policy under 15 U.S.C. § 57a.

[45] Courts recognize that consent decrees "'constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*.'" *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621 (D.N.J. 2014), *aff'd* No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (quoting *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis added by court)). *See supra* Argument, § 1.C.1.b (Mr. Kaufman's Testimony Did Not Violate the APA), at 68-69 for a discussion of consent agreements.

Indeed, the Commission is not required to promulgate "statements of general policy" or rules relating to data security before enforcing Section 5 of the FTC Act in the data security context. Comm'n Order Denying Resp't's Mot. to Dismiss at 14-15 (Jan. 16, 2014); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 619 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (finding that precedent does not "require[] the FTC to formally publish a regulation before bringing an enforcement action under Section 5's unfairness prong"); *POM Wonderful, LLC v. FTC*, 777 F.3d 478, 497 (D.C. Cir. 2015) (affirming that the Commission "validly proceeded by adjudication" and is not required to engage in rulemaking even where an administration decision may "affect agency policy and have general prospective application" (quotation marks and citations omitted)); *see SEC v. Chenery Corp.*, 332 U.S. 194, 202-03 (1947) (holding that agencies "must be equipped to act either by general rule or *by individual order*" and "retain power to deal with [] problems on a case-to-case basis if the administrative process is to be effective" (emphasis added)).[46]

The Commission validly proceeded by adjudication in this matter. The Supreme Court ruled that agencies "retain power to deal with [] problems on a case-by-case basis." *Chenery*, 332 U.S. at 203. This applies particularly where "the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule." *Id.* As the Commission recognized, "complex questions relating to data security practices in an online

[46] Respondent's reliance on *Util. Solid Waste Activities Grp. v. EPA.*, 236 F.3d 749 (D.C. Cir. 2001), is in error. That case involved EPA's amendment to a published rule without notice and comment. *Id.* at 752 ("On June 24, 1999, without notice and comment, EPA amended the PCB Mega Rule."). The court determined that EPA's amendment did not meet the standards for the APA's exceptions to notice and comment rulemaking. *Id.* at 754-55. Respondent's selective quotations, *see, e.g.*, Resp't's Post-Trial Brief at 61-62, do not transform *Utility Solid Waste Activities Group* into a mandate that the Commission publish statements of general policy.

environment are particularly well-suited to case-by-case development." Comm'n Order Denying Resp't's Mot. to Dismiss at 14 (Jan. 16, 2014); *see also* FTC, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf (noting that Congress "left the development of Section 5 to the Federal Trade Commission as an expert administrative body, which would apply the statute on a flexible case-by-case basis, subject to judicial review").

2. The Commission Has Not Violated the APA With Respect to Ex Parte Communication

Complaint Counsel addressed Respondent's arguments relating to alleged *ex parte* communication *supra*. Argument, § I.C.4.d (The Commission's Response to OGR's Request for Information Does Not Demonstrate Bias), at 83-85.

3. Complaint Counsel Has Proven that LabMD's Unreasonable Data Security Violated Section 5 and Was Not Offset by Countervailing Benefits

The harm caused or likely to be caused to consumers by LabMD's unreasonable data security practices was not offset by countervailing benefits to consumers or competition. *See infra*, Argument, § II.C.3 (Complaint Counsel Has Proven that LabMD's Unfair Practices Caused or Likely Caused Substantial Injury to Consumers That Was Not Outweighed by Countervailing Benefits to Consumers or Competition), at 128-31; *see generally* CCFF ¶¶ 1472-1798; CCCL ¶¶ 24-53.

Respondent asserts, without citing to evidence that describes the efficiency of LabMD's process in relation to pre-existing or competing processes, that "LabMD's business model offered groundbreaking benefits to doctors and patients, delivering pathology results to doctors

electronically at unprecedented speed." Resp't's Post-Trial Brief at 64. However, even if this were true, LabMD could have implemented many low cost security measures that would not have affected LabMD's ability to provide "groundbreaking benefits." *See* CCFF ¶¶ 1121-1185. In any event, countervailing benefits are determined based on the specific practice at issue in a complaint, in this instance unreasonable data security, not the overall operation of a business. *FTC v. Accusearch, Inc*., 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009) ("While there may be countervailing benefits to some of the information and services provided by 'data brokers' such as *Abika.com*, there are no countervailing benefits to consumers or competition derived from the specific practice of illicitly obtaining and selling confidential consumer phone records."); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (upholding Commission finding of no countervailing benefits because an increase in fees "was not accompanied" by an increased level or quality of service); *Apple, Inc.*, No. 112-3108, Statement of Comm'r Maureen K. Ohlhausen at 3 (Jan. 15, 2014) (reiterating that countervailing benefit determination is made by "compar[ing] that harm to any benefits from that particular practice").

4. Complaint Counsel Gathered and Presented Myriad Evidence of LabMD's Unreasonable Data Security Practices

Even assuming that the "Commission exercised enforcement authority based on information that Tiversa provided notwithstanding Tiversa's economic interest therein, and without independent verification that Tiversa's information was accurate," Resp't's Post-Trial Brief at 64, which it did not, the Commission did not violate the APA. The sole authority to which Respondent cites, *XP Vehicles*, stands only for the proposition that an APA claim survives a motion to dismiss where an agency's explanation for its decision was "mere pretext" for political cronyism, and where the agency's decision-making process was contrary to applicable

criteria set forth in agency regulations. *XP Vehicles, Inc. v. DOE*, No. 13-0037, 2015 U.S. Dist. LEXIS 90998, *94-*100 (D.D.C. July 14, 2015). *XP Vehicles* makes no reference to evaluating a third-party witness's economic interests, nor does it impose a requirement that an agency independently verify a third-party witness's information before initiating an investigation. Respondent offers no legal support – nor can it – for the proposition that it is a *per se* violation of the APA for an agency to fail to independently verify information received from a third party.

Again, even if Respondent's statement were true, it is not improper for an agency to act on information from a third party that may have a financial incentive for the agency to pursue the investigation. Agencies routinely act on information from third parties that may have ulterior motives in bringing a violation of the law to an agency's attention. *Osborne v. Grussing*, 477 F.3d 1002, 1007 (8th Cir. 2007) ("[R]egulatory and law enforcement agencies routinely act on the basis of information provided by private parties who harbor a grudge or who hope to benefit personally from their complaints, such as jealous competitors, disgruntled former employees, confidential informants, and cooperating co-conspirators. When such a complaint results in enforcement action, we do not impute the complainant's ulterior motive to the government enforcers."). Indeed, the idea that law enforcement benefits from individuals who may have ulterior, financial motivations is the predicate for the whistleblower provision of the False Claims Act, a program that resulted in the return of billions of dollars to the federal government. *See* Fraud Statistics – Overview, Oct. 1, 1987 - Sept. 30, 2013, Civil Division, U.S. Department of Justice, *available at* http://www.justice.gov/sites/default/files/civil/legacy/2013/12/26/C-FRAUDS_FCA_Statistics.pdf.

By contrast, the decision to enforce (or refrain from enforcing) a statute is committed to the agency's "absolute discretion." *Heckler v. Chaney*, 470 U.S. 821, 831 (1985). Unlike the

DOE's statutory and regulatory criteria for evaluating loan applications that were at issue in *XP Vehicles*, the FTC's unfairness program is limited only by the factors of 45 U.S.C. § 45(n), which have been established in this matter. CCFF ¶¶ 382-1177, 1354-1798. "If [Congress] has indicated an intent to circumscribe agency enforcement discretion, and has provided meaningful standards for defining the limits of that discretion, there is 'law to apply' under [the APA], and courts may require that the agency follow that law; if it has not, then an agency refusal to institute proceedings is a decision 'committed to agency discretion by law' within the meaning of [the APA]." *Heckler*, 470 U.S. at 834-35. Agencies exercising enforcement authority necessarily must have and use discretion to target particular companies, even if other, untargeted companies are engaging in similar practices. *Reese Bros. v. U.S. Postal Serv.*, 905 F. Supp. 2d 223, 257 (D.D.C. 2012) ("The failure to assess deficiencies against other mailers who were using the nonprofit rate while operating pursuant to similar contracts does not pose the same problem as agencies generally have broad discretion in the exercise of their enforcement powers.").

Finally, regardless of the genesis of this case, Complaint Counsel developed and presented myriad evidence that "independently verifies" that LabMD lacked reasonable data security. *See, e.g.*, CCFF ¶¶ 382-1110.

II. Complaint Counsel Has Proven Its Case

A. Complaint Counsel Has Proven the Elements of Section 5(n)

Respondent raises a number of arguments in bullet point fashion. Many of these arguments are duplicative and are addressed elsewhere in Complaint Counsel's brief, as described below. Respondent's remaining arguments are addressed in this section.[47]

Respondent's attempt to impose alternate definitions on the term "unfair," Resp't's Post-Trial Brief at 65,[48] is addressed *supra*, Burden of Proof/Standard of Review, at 40-41, (addressing claims relating to dictionary definitions and "generalized adverse impact"), as well as *infra* at Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 95-96 (addressing claims relating to "unjust, inequitable, or designed to exploit," acts or practices "are unfair to consumers generally and/or affected enough consumers to implicate or affect free and fair competition in the market generally").

Respondent's argument that Complaint Counsel must prove Respondent's unreasonable practices "cause[] substantial injury now," Resp't's Post-Trial Brief at 65, is addressed *supra*, Burden of Proof, § I (Complaint Counsel's Burden of Proof is Defined by Section 5), at 44.

Complaint Counsel addresses Respondent's assertion that Section 5 limits the Commission to pursuing a single unfair act or practice committed by a respondent below.

---

[47] For the convenience of the reader, Complaint Counsel has addressed each of the bullet points in summary fashion with appropriate references. Complaint Counsel's responses to the bulleted arguments not otherwise addressed appear below in subsections 1 through 4.

[48] Respondent offers variously that unfair means "unjust, inequitable, or designed to exploit," "unfair to consumers generally," or "implicate[s] or affect[s] free and fair competition in the market generally." Resp't's Post-Trial Brief at 65, 68.

Argument, § II.A.1 (The Commission is Not Limited to Pursuing An Action for a Single Act or Practice), at 94-95.

Respondent's argument that Complaint Counsel must prove that its unreasonable acts or practices are likely to recur,[49] Resp't's Post-Trial Brief at 66, is addressed *supra*, Burden of Proof, § I (Complaint Counsel's Burden of Proof is Defined by Section 5), at 42-43.

Respondent's claim that Section 5's standard of proof requires an "actual data breach," Resp't's Post-Trial Brief at 66, is addressed *infra*, Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 96; *see also supra* Burden of Proof, § II (Section 5(n) Sets Forth Complaint Counsel's Burden of Proof on Injury), at 46-47.

Respondent's claim that Complaint Counsel must prove consumer injury that is "substantial, tangible and more than merely speculative," Resp't's Post-Trial Brief at 67, is addressed below. Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 96-97.

Respondent's assertion that an ability to mitigate harm after the fact – a fact that is counter to the evidence, *see, e.g.*, CCFF ¶¶ 1502-1503 (notifications do not remediate all consumer harms), 1570-1575 (SSNs are valuable to identity thieves for a long period of time), 1612-1618 (health injury due to medical identity theft), 1695-1697 (reputational harm) – obviates a violation of Section 5(n) is addressed below. Argument, § II.A.3 (Consumers Could Not Reasonably Avoid Injury Caused or Likely Caused by LabMD), at 99-100.

---

[49] For a discussion of Respondent's contention that "likely" means "highly or even merely probable," see *supra*, Burden of Proof § I (Complaint Counsel's Burden of Proof is Defined by Section 5(n)), at 44-45.

Respondent's attempt to add yet another element to Section 5(n), that harms be widespread or unfair to the public generally, is discussed below. Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury).

Respondent's argument that Complaint Counsel must prove that LabMD's unfair acts or practices posed an obstacle to the free exercise of consumer decisionmaking, Resp't's Post-Trial Brief at 65, 68, are addressed *supra*, Burden of Proof, § II (Section 5(n) Sets Forth Complaint Counsel's Burden of Proof on Injury), at 47.

Respondent's argument's relating to Complaint Counsel's burden of proving that the harm caused or likely caused by its unreasonable acts or practices was not outweighed by countervailing benefits, Resp't's Post-Trial Brief at 68, is addressed *infra*, Argument, § II.C.3 (Complaint Counsel Has Proven that LabMD's Unfair Practices Caused or Likely Caused Substantial Injury to Consumers That Was Not Outweighed by Countervailing Benefits to Consumers or Competition), at 128-31.

Respondent's claim related to its alleged reliance on IT experts is addressed *infra*. Argument, § II.C.4 (LabMD Had Control Over and Was Responsible For its Own Unreasonable Data Security), at 131-33; *see also supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 5-8.

Complaint Counsel addresses the inapplicability of the OSHA General Duty Clause to Section 5 *infra*, Argument, § II.A.4 (Section 5 is Not Modified by OSHA), at 100-01.

1. The Commission Is Not Limited to Pursuing an Action for a Single Act or Practice[50]

Respondent's argument that Section 5 allows the Commission to declare unlawful only a single action at a time is absurd. Resp't's Post-Trial Brief at 65-66. Focusing only on Section 5(n)'s definition of what constitutes an unlawful act or practice, Respondent ignores Section 5's operative sections which declare "unfair or deceptive act*s* or practices" unlawful (15 U.S.C. § 45(a)(1)) and give the Commission the power to prevent "unfair or deceptive act*s* of practice*s*." (15 U.S.C. § 45(a)(2)) (emphases added). *See also, e.g.*, *FTC v. Neovi*, 604 F.3d 1150, 1153 (9th Cir. 2010) ("The Federal Trade Commission . . . has broad powers under the FTC Act to prevent businesses from engaging in unfair or deceptive practice*s*."); *id.* at 1155-56 (upholding companies' liability for both creating *and* delivering unverified checks in an unfair manner) (emphasis added). The unsurprising fact that the requirements for finding any particular act or practice unreasonable in Section 5(n) uses singular nouns does not somehow undo the grant of authority in Section 5(a). Respondent's argument cannot be supported by a plain reading of the statute, is completely without legal authority, and is facially absurd. *See Clinton v. City of New York*, 524 U.S. 417, 429 (1998) (interpretations of statutes that create absurd and unjust results are to be avoided).

2. Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury

Complaint Counsel has met its burden to prove by a preponderance of evidence that LabMD's unreasonable security practices caused or are likely to cause substantial injury to consumers. 15 U.S.C. § 45(n); CCRRFF ¶ 480; CCCL ¶¶ 3, 21, 24-27; JX0001-A at 3. Each of

---

[50] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

Respondent's attempts to offer additional or alternative legal tests to the burden of proof under Section 5 fails.

First, Respondent's statements that unfairness under Section 5 requires Complaint Counsel to prove that Respondent's practices are "unjust, inequitable, or designed to exploit," that the acts or practices "are unfair to consumers generally and/or affected enough consumers to implicate or affect free and fair competition in the market generally," or that the harm it caused must be "widespread" or "unfair to the public generally," Resp't's Post-Trial Brief at 65, 68, 70; CCRRCL ¶¶ 47, 60, are baseless and not supported by any authority. As the Commission held, Section 5(n) fully defines the elements of unfairness under Section 5, and provides adequate constitutional notice. Comm'n Order Denying Resp't's Mot. to Dismiss 16-19 (Jan. 16, 2014); *see also* JX0001-A at 3 (stipulating that "Complaint Counsel has the burden of proof to prove by a preponderance of evidence that LabMD's practices are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."). Any ambiguity in the term unfairness was resolved by the codification of Section 5(n). Respondent cannot add limitations to the definition of unfairness other than those found in Section 5(n). *See* CCRRCL ¶¶ 47, 60.

Second, Respondent grossly misrepresents the law of this case in asserting that "an actual data breach" is necessary for a Section 5(n) violation. Resp't's Post-Trial Brief at 66 (bulleted argument), 70-71 (text). In fact, the Commission stated the *opposite*, on one of the very pages Respondent cites for its proposition: "occurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted unfair . . . acts or practices." Comm'n Order Denying Resp't's Mot. to Dismiss 19 (Jan. 16, 2014) (internal

quotations and citations omitted); *see also FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *6 (3d Cir. Aug. 24, 2015) ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."). Respondent's citations to Section 5(n), *Wyndham Worldwide Corp.*, and the Unfairness Statement also fail to support this assertion. *See* CCRRCL ¶ 78. As the Commission stated, whether "actual data breaches" occurred is not dispositive of anything. Regardless, Respondent does not—and cannot—support its argument that the Security Incidents alleged in this complaint are not "actual data breaches." Resp't's Post-Trial Brief at 71. Particularly in cases involving breaches of sensitive information that reveals private, personal characteristics, as this one does, CCFF ¶¶ 1684-1697, mere disclosure of the information causes substantial harm.

Third, Respondent's assertion that "Complaint Counsel must allege and prove by a preponderance of the evidence a consumer injury that is substantial, tangible and more than merely speculative" is a misstatement of Complaint Counsel's burden. Resp't's Post-Trial Brief at 67. Section 5(n), which requires proof that an act or practice caused or is likely to cause substantial injury, is the beginning and the end of Complaint Counsel's burden of proof, Comm'n Order Denying Resp't's Mot. to Dismiss 16-19 (Jan. 16, 2014); JX0001-A at 3, and Complaint Counsel has met it. CCCL ¶¶ 29-40. Furthermore, the Unfairness Statement to which Respondent repeatedly cites, Resp't's Post-Trial Brief at 68-70, is consistent with Section 5(n), and does not impose additional burdens. *See Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290, at *97 (1984) (unfairness statement); *see also id.* at *101 n.12 (a practice is unfair if it causes or is likely to cause "a small amount of harm to a large number of people, or if it raises a significant risk of concrete harm"); Comm'n Order Denying Resp't's Mot. to Dismiss 18-19

(Jan. 16, 2014). In any case, the injury and likelihood of injury Complaint Counsel has proven in this case is not speculative, and satisfies the standard of Section 5(n). CCRRCL ¶ 80.

Fourth, the burden of proving injury-in-fact to establish Article III standing has no bearing on the burdens of proof in this proceeding, and LabMD has provided no authority showing otherwise. CCRRCL ¶ 81; *see* Resp't's Post-Trial Brief at 67 (bulleted argument), 72 (text). The Commission is not required to prove standing. CCRRCL ¶ 81. And for good reason. The Commission's posture differs from that of an individual litigant. *See* CCCL ¶¶ 24-25, 31, 34. The Commission is authorized to prevent persons from using unfair acts or practices, even those that are "likely to cause substantial injury." 15 U.S.C. § 45(b), (n). And the Commission does not need to wait for harm to manifest before challenging conduct. CCCL ¶ 25; *see also FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *6 (3d Cir. Aug. 24, 2015) ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."). Likewise, the Commission's Order on the Motion to Dismiss disposed of Respondent's argument that "where no misuse is proven there has been no injury as a matter of law." Comm'n Order Denying Resp't's Mot. to Dismiss 19 (Jan. 16, 2014); CCRRCL ¶ 82. The *Reilly v. Ceridian Corp.* decision cited by Respondents is limited to the Article III standing context and is factually and legally inapplicable in this matter. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 41-43, 46 (3d Cir. 2011); CCRRFF ¶ 82.

Finally, Complaint Counsel has met its burden of proving that LabMD's practices caused or are likely to cause substantial injury in this case. CCCL ¶¶ 29-40. Complaint Counsel has not "abandoned" the 1718 File as Respondent asserts. Resp't's Post-Trial Brief at 66 n.13. Although Complaint Counsel did not rely on the testimony of Mr. Boback, or any expert testimony or opinions based on that testimony, the record is uncontroverted that LabMD was

sharing the 1718 File on a public P2P network, through LimeWire installed on its billing manager's computer, JX0001-A at 3; CCFF ¶ 1393, and that a Tiversa employee was able to locate the file and download it using an off-the-shelf peer-to-peer client, CCFF ¶ 1394. Accordingly, the record does not support the assertions that the 1718 file "never left Atlanta, Georgia," CCRRFF ¶¶ 482, 485, 484, or that "no consumer ever could likely be substantially harmed," CCFF ¶¶ 1472-1798. As described further below, the injury caused or likely to be caused by LabMD's practices rises far above "speculation about possible identity theft and fraud." Resp't's Post-Trial Brief at 71; *see* CCRRCL ¶¶ 80, 206. LabMD's failures caused or are likely to cause substantial injury to consumers. CCFF ¶¶ 1472-1798.[51]

3. Consumers Could Not Reasonably Avoid Injury Caused or Likely Caused by LabMD

Respondent's argument that harm is reasonably avoidable if a consumer can mitigate the harm suffered, even if that mitigation is costly and incomplete, is erroneous. A consumer that is required to expend time and money to remediate harm caused by a party's actions cannot be said to have avoided injury. CCCL ¶ 35. At least one court has specifically rejected Respondent's argument. *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010). In *Neovi*, the defendant argued that because consumers could mitigate the harm caused by defendant's actions after the harm had occurred then the injury was reasonably avoidable and did not satisfy Section 5(n). *Id.* at 1158. The Court rejected this argument, adopting the trial court's holding that injury was not reasonably avoidable where some consumers might be unaware of the injury, and the consumers that did notice the injury could mitigate the harm only through a "substantial investment of time,

[51] Contrary to Respondent's representation, Dr. Hill did not opine that LabMD's physical security in general was adequate. CCRRFF ¶ 297 (quoting Hill, Tr. 293). She opined on the

trouble, aggravation, and money." *Id.*; *cf. FTC v. Direct Benefits Group, LLC*, No. 6:11-cv-1186, 2013 WL 3771322, at *14 (M.D. Fla. July 18, 2013) ("[T]he fact that many customers were able to—eventually—obtain refunds from Defendants does not render the injury avoidable.").

Complaint Counsel has proved that consumers could not reasonably avoid injury caused or likely caused by LabMD's unreasonable data security. As in *Orkin*, "[a]nticipatory avoidance through consumer choice was impossible" in this case because consumers had no way of knowing that LabMD would receive their specimen and Personal Information, and had no way of knowing LabMD's unreasonable security practices. *Orkin Exterminating Co. v. F.T.C.*, 849 F.2d 1354, 1365 (11th Cir. 1988); CCFF ¶¶ 1777-1787; *cf. FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (finding no countervailing benefits where consumers "did not give their consent to enrollment in OnlineSupplier, and thus, the harm resulted from a practice for which they did not bargain"); *see also* CCCL ¶¶ 42-44.

Respondent's reliance on *Davis v. HSBC Bank Nevada*, 691 F.3d 1152 (9th Cir. 2012), is misplaced. CCRRCL ¶ 83. *Davis* involved a putative class action in which the individual plaintiff sought relief under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"). *Id.* at 1158-59. To be unlawful under the UCL practices must violate another law. *Id.* at 1168. Davis argued that the challenged practice, charging an annual fee on a credit card without sufficient notice, violated 12 C.F.R. § 7.4008(c), which prohibits national banks from engaging in unfair or deceptive practices as defined in Section 5 of the FTC Act. *Id.* at 1168. The *Davis* court concluded that the plaintiff could have reasonably avoided the annual

---

adequacy of only two narrow components of its physical security that related directly to network security. CCRRFF ¶ 297.

charge by simply reading the terms and conditions of the credit card before applying for the credit card, or by canceling within 90 days after signing up for the credit card. *Id*. at 1169. Such an analysis does not apply in this case, where consumers would have no way of avoiding the injury prior to the injury, no reliable way of learning of the injury, and no reliable way to mitigate the harm after any injury occurred. *See* CCFF ¶¶ 1708-1711,1773-1774, 1785-1787.

4. Section 5 is Not Modified by OSHA

The enforcement of OSHA's General Duty Clause does not constrain the Commission's enforcement of Section 5, nor could it. Respondent attempts to turn Complaint Counsel's "analogy" cited for one purpose (the consideration of several factors in determining reasonableness in the enforcement of OSHA's General Duty Clause in Department of Labor administrative courts) into "equivalence" for another purpose (to change the burden of proof under Section 5(n)). Respondent may not rewrite the law. As discussed below, reasonableness is the applicable test, *infra* Argument, § II.C.1. (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27 and Section 5(n) itself sets forth the standard of proof for the Commission to find an act or practice "unfair," *infra* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

OSHA's legal framework and requirements are inapposite to the unfairness analysis set forth in Section 5(n). Therefore, the OSHA cases cited by Respondent are irrelevant the FTC's application of Section 5. Unlike in the FTC context, in the OSHA statute, Congress directed the Secretary of Labor to promulgate and establish new standards. *See* 29 U.S.C. § 655(a), (b)(1)-(4) (directing the Secretary of Labor to "promulgate as an occupational safety or health standard any national consensus standards, and any established Federal standard" within two years of OSHA's enactment and to engage in notice and comment rulemaking thereafter to establish new

standards). Congress gave the FTC broad discretionary authority to define unfair practices on a flexible and incremental basis, and the FTC Act contains no similar rulemaking directive. *See* 15 U.S.C. Ch. 2; *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985).

Furthermore, there is no distinct "medical data security reasonableness" under Section 5. *Infra* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41. Rather, using its broad discretionary authority, the Commission analyzes the adequacy of security practices companies use to protect information, including medical information using the reasonableness test, *see infra* Argument, § II.C.1 (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27, in determining whether acts or practices are unfair in violation of Section 5.

Finally, as discussed below all entities, including Respondent, had adequate notice of its duty to provide reasonable data security. *Infra* Argument, § II.C.1 (Section 5 Gives Fair Notice of its Proscriptions), at 125-27.

B. Complaint Counsel's Experts Provided Competent and Reliable Testimony[52]

The Court should disregard LabMD's latest attempt to exclude or diminish the weight of opinions offered by Complaint Counsel's experts in this case, Dr. Raquel Hill, Mr. James Van Dyke, and Mr. Rick Kam. Each of these experts is qualified in a relevant field under *Daubert* and Federal Rule of Evidence 702. Each of these experts provided opinions based on reliable methodology applied to the facts of this case. Each of these experts provided opinions that will be helpful to the Court in deciding key disputed issues. Each of these experts testified at trial

---

[52] Respondent includes an argument in this section claiming that reasonable data security differs for the medical industry. This argument is addressed *infra*, Argument, §§ II.C.1 (Section 5 Gives Fair Notice of its Proscriptions), at 125-27, and II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

and the opinions offered were vetted through vigorous cross-examination and the presentation of contrary evidence. In its post-trial brief, LabMD now broadly seeks to exclude or limit certain of Complaint Counsel's experts' opinions as "lack[ing] scientific and factual credibility." But LabMD has failed to show that any of the challenged expert opinions that Complaint Counsel relies on are clearly inadmissible under *Daubert* or not entitled to the Court's full consideration. The Court should decline LabMD's invitation and instead consider the expert opinions of Dr. Hill, Mr. Van Dyke, and Mr. Kam that Complaint Counsel relies on along with all other evidence in this case. [53]

1. Dr. Hill's Opinions are Reliable and Will Provide Valuable Assistance to the Court

LabMD challenges Dr. Hill's methodology and opinions regarding LabMD's data security practices on several broad grounds. Specifically, LabMD contends that: (i) the methodology for implementing a layered defense strategy is not reliable, Resp't's Post-Trial Brief at 75; (ii) opinions on data security standards do not consider the size and nature of LabMD's business or FTC guidelines and do not "fit" this case, Resp't's Post-Trial Brief at 75, 77-79; (iii) LabMD lacked notice of how to implement a layered defense strategy during the relevant time period, Resp't's Post-Trial Brief at 76; and (iv) certain opinions are based on unreliable fact testimony, Resp't's Post-Trial Brief at 76-77. LabMD's arguments are meritless

---

[53] In a footnote, LabMD states that it is renewing its oral and written *Daubert* motions regarding Dr. Hill, Mr. Van Dyke, and Mr. Kam (Resp't's Post-Trial Brief at 74, n.16). To the extent the Court wishes to revisit prior oral and written *Daubert* motions in this case, Complaint Counsel hereby renews, as fully incorporated herein, its oral and written opposition to LabMD's prior *Daubert* motions. *See* Hill, Tr. 325-330; Van Dyke, Tr. 741-744; Complaint Counsel's Opposition to Respondent's Motion *In Limine* To Exclude Expert Testimony of James Van Dyke, dated April 29, 2014; Kam, Tr. 569-573; Complaint Counsel's Opposition to Respondent's Motion *In Limine* to Exclude Expert Testimony of Rick Kam, dated April 29, 2014.

and should be rejected. Contrary to LabMD's assertions, Dr. Hill has offered reliable opinions assessing whether LabMD provided reasonable security for Personal Information within its computer network, and whether any security failures could have been corrected using readily available security measures during the relevant time period. CCFF ¶ 19. Dr. Hill's opinions will assist the Court in this case and should be considered in full.

i. Dr. Hill's Methodology For Implementing a Layered Defense Strategy is Reliable

Dr. Hill, a tenured professor of Computer Science at Indiana University, is an expert in data security. CCFF ¶ 16. Dr. Hill holds a Ph.D. in Computer Science from Harvard University and has over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems. CCFF ¶¶ 16-17. Based on a thorough review of the facts of this case and her experience and professional qualifications, Dr. Hill opined that companies should consider certain key principles in developing and implementing a layered defense strategy to protect their computer networks and the information on them. CCFF ¶ 394. Those key principles include: (1) Don't keep what you don't need; (2) Patch software; (3) Close unused ports; (4) Create and implement security policies; (5) Protect the network with security software; (6) Probe the network with periodic audits, including penetration testing; and (7) Create and implement policies that govern the physical access to devices and data. CCFF ¶ 394.

LabMD contends these principles are not reliable but its position is unsupported. Resp't's Post-Trial Brief at 75 (citing Hill, Tr. 242-243). LabMD's primary argument is that Dr. Hill did not identify one document as the source of the seven principles. This is untenable. Dr. Hill has provided uncontroverted testimony that she relied on widely known and accepted guidance from multiple sources to formulate her opinions regarding key principles companies

should consider when implementing a layered defense strategy. Hill, Tr. 242-245; CCFF ¶ 394; CX0740 (Hill Report) at 64-65. Dr. Hill's opinion that using multiple, layered security measures satisfies the reasonableness test for securing a network containing sensitive personal information and the information on it is entirely consistent with security standards that were well known during the relevant time period. For example, NIST Special Publication 800-30, dated July 2002, identifies the risk management process for data security as encompassing risk assessment, risk mitigation, and evaluation and assessment. CX0400 (NIST Special Publication 800-30) at 11.[54] There is no question about the general applicability of the practices set out in CX0400, which LabMD failed to observe. *See* CCFF ¶¶ 483-810 (LabMD did not use appropriate measures to assess risk); CCFF ¶¶ 811-827 (LabMD did not prevent employees from accessing Personal Information not needed to do their jobs); CCFF ¶¶ 527-629 (LabMD did not adequately update, run, or review antivirus software and scans); CCFF ¶¶ 960-963 (LabMD did not prevent employees from sharing authentication credentials). Moreover, as Dr. Hill explained, concepts

[54] NIST identified many types of threats to computer systems, such as a firewall allowing guest access to a server without username and password login, failure to apply patches to a system, and failure to remove terminated employees' identifiers from a system. (CX0400 (NIST Special Publication 800-30) at 22-23; *see* CCFF ¶¶ 759-771 (LabMD's Mapper server allowed write access to the root directory by users without credentials); CCFF ¶¶ 996-1040 (LabMD did not patch and update operating systems and other programs); CCFF ¶¶ 986-987 (LabMD did not deactivate the login access of former clients, and Ms. Simmons's credentials remained valid a year after she left LabMD)). NIST also recommended that companies develop security requirements for technical security based on many criteria, including security of communications, cryptography (encryption), discretionary access control, identification and authentication, and intrusion detection. (CX0400 (NIST Special Publication 800-30) at 26; *see* CCFF ¶¶ 452-454 (LabMD's Policy Manuals did not have policies describing how information would be protected in transit and whether sensitive information would be stored in an encrypted format), 474-480 (LabMD did not provide tools to allow employees to encrypt emails containing sensitive data); CCFF ¶¶ 811-827 (LabMD did not implement mechanisms to restrict employee access to information not needed to do their jobs); CCFF ¶¶ 909-983 (LabMD did not have or enforce policies requiring strong passwords); CCFF ¶¶ 699-702 (LabMD did not implement an intrusion detection or protection system)).

such as patching software, closing unused ports, and specifying strong password policies "are captured in general guidelines" and "are very basic recommendations that anyone would use to protect their infrastructure." Hill, Tr. 245.

LabMD next argues there is no evidence to suggest the principles Dr. Hill relies on were "subject to testing or peer review." Resp't's Post-Trial Brief at 75. This argument also fails. As discussed above, Dr. Hill has provided uncontroverted testimony that she relied on widely known and accepted guidance from multiple sources to formulate the opinions LabMD now challenges. Hill, Tr. 242-245; CCFF ¶ 394; *see Bitler v. A.O. Smith Corp.*, 400 F.3d 1227, 1235 (10th Cir. 2004) (holding that expert's methodology was reliable as it was generally accepted, despite a lack of testing or peer review). Moreover, Dr. Hill's extensive experience working in the field of data security, as well as her knowledge of and reliance on relevant literature concerning data security, confirm her opinions are reliable and should be considered here. *See Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 593-95 (1993) ("The inquiry envisioned by Rule 702 is, we emphasize, a flexible one"); *Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137, 150-51 (1999) (*Daubert* factors are "meant to be helpful, not definitive"); Fed. R. Evid. 702 advisory committee's note (2000 Amendment) (noting that when an expert relies "primarily on experience, then the witness must explain how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts"); *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC*, 691 F. Supp. 2d 448, 473 (S.D.N.Y. 2010) (applying advisory committee note's standard for experience qualifying an expert).

ii. Dr. Hill Properly Analyzed Data Security Standards as Applied to LabMD and Her Opinions Fit the Facts of This Case[55]

Dr. Hill has offered expert opinions on industry standards relating to computer security and information technology as applied to the facts of this case. Hill, Tr. 234-235. LabMD has challenged these opinions on the grounds that data security standards applicable to entities like LabMD that hold medical information are different, and Dr. Hill's opinions therefore do not "fit" the facts of this case. Resp't's Post-Trial Brief at 75, 78-79.[56] LabMD has also criticized Dr. Hill's opinions on the ground that she did not consider FTC standards and guidelines. Resp't's Post-Trial Brief at 77-78. LabMD's arguments are meritless and should be rejected.

Respondent's rehashed and rejected argument claiming a different data security standard for the medical industry is the same failed argument Respondent made to the Commission: that "HIPAA's comprehensive framework governing 'patient-information data-security practices' by HIPAA-regulated entities somehow trumps the application of the FTC Act to that category of practices." Comm'n Order Denying Resp't's Mot. to Dismiss at 11-12 (Jan. 16, 2014) (internal citation omitted). The Commission already rejected that argument, stating, "HIPAA evinces no congressional intent to preserve anyone's ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act, and enforcement of that Act thus fully comports with congressional intent under HIPAA." *Id.* at 12. "The Commission

---

[55] Complaint Counsel has combined its response to Respondent's related brief sections Argument, II.B.1.ii, at 75, II.B.1.v, at 77-78, and II.B.1.vi, at 78-79 in this subsection.

[56] Rule 702 requires that expert testimony must fit the issues in the case, meaning it "must be relevant for the purposes of the case and must assist the trier of fact." *Schneider ex rel. Estate of Schneider v. Fried*, 320 F.3d 396, 404 (3d Cir. 2003).

cannot enforce HIPAA and does not seek to do so. But nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act." *Id.* at 12.

Contrary to LabMD's assertions, the industry standards Dr. Hill has opined on apply to exactly the type of data LabMD holds. (Hill, Tr. 234-235; CX0740 (Hill Report) at 64-66). LabMD holds Personal Information of the type held by organizations operating in many industries, such as names, dates of birth, Social Security numbers, and financial accounts numbers. (JX0001-A (Joint Stips. of Fact, Law, & Authenticity) at 1-2.[57] Further, as Dr. Hill testified, she took into account recommendations, guidelines, and best practices from a wide variety of organizations across industries in forming her opinions. (CX0740 (Hill Report) at 66).[58] Moreover, Dr. Hill explained that for purposes of protecting computer networks, and their equipment and information, common guidelines are applied to protect across all industries, including to protect medical data. Hill, Tr. 234-235 ("A: … Computing is pervasive, so these guidelines, whether they're from NIST or from the Computer Emergency Response Team or from the National Research Council that specifically focused on medical data, they have consistent guidelines. And that's because computing is pervasive and consistent across different

---

[57] LabMD also holds additional sensitive information relating to consumers' health. *Id.* This fact is relevant to the level of protection that LabMD must reasonably provide to data under its control, but does not dictate any particularized standard. LabMD's reliance on *S&H Riggers & Erectors Inc. v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981) is misplaced. Complaint Counsel has addressed Respondent's arguments raised at pages 78-79 of its brief claiming that reasonable data security differs for the medical industry *infra*, Argument, §§ II.C.1 (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27, and II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

[58] National Research Council, "For the Record: Protecting Electronic Health Information" Washington, DC: The National Academies Press (1997), http://www.nap.edu/openbook.php?record id=5595&page=R1, last accessed Mar. 16, 2014.

types of business domains."); RX0524 (Hill, Dep. at 61-62 ("A: … these are standards that are used across … different types of industries as it relates to computer security"). LabMD offers no relevant evidence to rebut this testimony. Resp't's Post-Trial Brief at 75.[59]

Nor is there any merit to LabMD's suggestion that HIPAA may alter the standard LabMD is held to when evaluating its data security practices. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); *see also* Comm'n Order Denying Resp't's Mot. for Summary Decision at 5-6 (May 19, 2014). Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. CX0765 (Resp't's Resps. to Compl. Counsel's Second Set of Discovery) at 12-13, Response to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence").

Finally, LabMD's complaint that Dr. Hill did not consider FTC materials in forming her opinions should be rejected. These materials merely summarize already well-known security practices included in various materials, including those Dr. Hill considered. The gravamen of the Complaint in this case is not failure to comply with "the FTC's widely available and known standards and guidelines regarding data security," as LabMD suggests. Resp't's Post-Trial Brief at 78. Rather, the Court will decide whether LabMD's multiple failures to provide reasonable

---

[59] The unremarkable fact that Dr. Hill has not "worked for a medical provider or lab" does not impact the weight of Dr. Hill's testimony and LabMD has failed to show otherwise. Resp't's Post-Trial Brief at 75. Indeed, it cannot, because the Section 5 inquiry is necessarily fact-bound, requiring consideration of case-specific facts in light of the statutory unfairness standard. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 16-18 (Jan. 16, 2014).

security for the Personal Information it collected and maintained violate the provisions of the Federal Trade Commission Act. Based on her review of materials cited and extensive professional experience, CCFF ¶¶ 16-18, Dr. Hill has provided reliable opinions that will assist the Court in understanding what constitutes reasonable data security practices.

iii. Layered Data Security Strategies Were Well Known During the Relevant Time Period

LabMD engaged in a number of practices that, taken together, failed to provide reasonable security for Personal Information on its computer networks. CCFF ¶ 382. As Dr. Hill has explained, a layered data security strategy is the most effective way to provide reasonable security for a network, its computers, and the information it stores. CCFF ¶¶ 384-395. LabMD argues that Dr. Hill was unaware of layered data strategy principles before 2009 and therefore LabMD could not have been expected to comply with these concepts any earlier. Resp't's Post-Trial Brief at 76. LabMD's entire argument, however, rests on cherry-picked testimony taken out of context.

Concepts for implementing a layered data security strategy were widely available to LabMD from many sources before 2009, and Dr. Hill reviewed such recommendations in preparing her report.[60] CX0740 (Hill Report) at 64-66. As discussed above, the National Institute For Standards and Technology ("NIST"), published a standard that explained the risk management process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level in 2002. CCFF ¶ 490; CX0400. Beginning in 2002, NIST Special Publication

[60] As discussed above, Dr. Hill opined that companies should consider certain key principles when implementing a layered defense strategy to protect their computer networks, including: (1) Don't keep what you don't need; (2) Patch software; (3) Close unused ports; (4) Create and implement security policies; (5) Protect the network with security software; (6) Probe the

800-30 (Risk Management Guide for Information Technology Systems) explained a nine step process, beginning with cataloging network resources (including hardware, software, information, and connections) to define the scope of risk assessment, moving through vulnerability identification and cost-benefit analyses of measures that could mitigate the risk of a vulnerability, and ending with security measure recommendations and a written record of the process. CCFF ¶ 491. These primary steps included methods and tools that could be used to perform them. CCFF ¶ 492.[61] Based on available general industry guidance and guidance specific to the medical industry during the relevant time period, LabMD knew or should have known to implement multiple controls and protections for Personal Information it held.

iv. Dr. Hill Properly Relied on Fact Testimony of Former LabMD Employee Curt Kaloustian

LabMD incorrectly contends that five statements in Dr. Hill's expert report are unreliable because they cite only to fact testimony that former employee Mr. Kaloustian provided at his investigational hearing deposition.[62] Resp't's Post-Trial Brief at 76-77. Respondents cite to no evidence controverting the facts Mr. Kaloustian testified to in the five statements it identifies. Resp't's Post-Trial Brief at 76-77. The factual testimony provided by Mr. Kaloustian at his May 3, 2013 investigational hearing was reliable and it is appropriate for Dr. Hill to rely on his

---

network with periodic audits, including penetration testing; and (7) Create and implement policies that govern the physical access to devices and data. CCFF ¶ 394.

[61] Other sources of guidance include the System Administration, Networking, and Security Institute ("SANS") security training and materials for practitioners who maintain and operate computer systems, and vulnerability information from the Global Information Assurance Certification organization ("GIAC"). (CCFF ¶¶ 494-495).

[62] Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony.

testimony in her expert report. Mr. Kaloustian testified under oath pursuant to a lawful CID, and he verified that his testimony was truthful, he answered all questions fully, and he cooperated with the CID. CX0735 (Kaloustian, IHT at 7 (witness sworn), 307). As explained supra, Argument, § I.C.3 (LabMD's Privileges Were Respected at Mr. Kaloustian's Investigational Hearing), at 74-78, the investigational hearing of Mr. Kaloustian was proper and did not violate due process.

Mr. Kaloustian was the primary employee in charge of LabMD's network whose responsibilities included maintaining the network architecture, maintaining the servers, patches, upgrades, and building the interfaces for client data, CCFF ¶¶ 350, and he had the greatest knowledge of LabMD's network during the time-period examined by Dr. Hill. In some instances, he was the *only* employee who had knowledge of certain aspects of LabMD's networks. *See, e.g.*, CX0730 (Simmons, Dep. at 16, 125-126) (Kaloustian was only employee who managed firewall limiting Internet access). As Alison Simmons, his contemporary as a LabMD IT employee, testified, Mr. Kaloustian was in charge of hardware, servers, and networks. CX0734 (Simmons, IHT at 57). Mr. Kaloustian was in charge of network security. CX0734 (Simmons, IHT at 86-87). Mr. Kaloustian would have been responsible for monitoring outbound traffic on LabMD's network. CX0730 (Simmons, Dep. at 156); CX0734 (Simmons, IHT at 161). Mr. Kaloustian managed the firewalls, both hardware, CX0730 (Simmons, Dep. at 16, 125-126); CX0734 (Simmons, IHT at 21), and software, CX0734 (Simmons, IHT at 104-105). It was his responsibility to maintain the servers. CX0734 (Simmons, IHT at 33-35, 169-170). Mr. Kaloustian and Ms. Simmons determined how to protect desktop computers. CX0734 (Simmons, IHT at 75). Mr. Kaloustian installed antivirus software on employee laptops. CX0734 (Simmons, IHT at 115-116, 119-120). Mr. Kaloustian cleaned up infected computers at

physician-clients' offices. CX0734 (Simmons, IHT at 103-04). The backups also were Mr. Kaloustian's responsibility. CX0734 (Simmons, IHT at 54-55, 164).

Moreover, it is appropriate for Dr. Hill to rely on Mr. Kaloustian's testimony because it is corroborated by other evidence in the record. For example:

- Penetration testing was never done. CCFF ¶¶ 715-726; CX0734 (Simmons, IHT at 67-68); *see also* CX0735 (Kaloustian, IHT at 92, 281-82).
- Firewalls were disabled on servers that contained personal information. CX0731 (Truett, Dep. at 79) (APT did not actively monitor the operation of LabMD's firewalls); CCFF ¶¶ 182-190 (APT); *cf.* CX0730 (Simmons, Dep. at 53-54), CX0734 (Simmons, IHT at 101-102) (firewalls disabled on desktops)); *see also* CX0735 (Kaloustian, IHT at 293-94).
- Personal Information was transmitted and stored in an unencrypted format. CX0734 (Simmons, IHT at 43); *see also* CX0735 (Kaloustian, IHT at 62-64, 302-04).
- LabMD's firewalls were not configured to prevent unauthorized traffic from entering the network. CX0730 (Simmons, Dep. at 53-54); CX0734 (Simmons, IHT at 100-02) (firewalls operated only to prevent employees from accessing some websites, but LabMD did not limit the web sites that Michael Daugherty, John Boyle, IT staff, the lab manager, the billing manager, and the pathologist could visit online); CCFF ¶¶ 1103-1104; CX0067 (ProviDyn Network Security Scan-LabNet) at 6, 22) (the external vulnerability scans that ProviDyn conducted in May 2010 indicate that port 10,000 was open); *id.* at 22 (the ProviDyn external vulnerability scans show that not only was port 10,000 open in 2010, but also that

LabMD's Veritas backup application had not been updated to correct buffer overflow the vulnerability that Symantec, the vendor, had identified); *see also* CX0735 (Kaloustian, IHT at 98-104).

Mr. Kaloustian testified under oath pursuant to a lawful CID, he verified that his testimony was truthful, he answered all questions fully, and he cooperated with the CID. CX0735 (Kaloustian, IHT at 7 (witness sworn), 307). Nothing in the testimony cited in the five statements in Dr. Hill's report is unreliable. Mr. Kaloustian was the primary employee responsible for LabMD's network and his testimony is corroborated by other witnesses and evidence. Moreover, Respondent failed to identify any contrary evidence to rebut Mr. Kaloustian's fact testimony, despite ample opportunity to do so. Additionally, if Respondent believed that any of Mr. Kaloustian's testimony was unreliable, it had the opportunity during discovery to depose Mr. Kaloustian on his previous testimony. Respondent chose not to do so. For all of these reasons, the Court should disregard Respondent's request and consider all aspects of Dr. Hill's report, along with all other evidence in the record.

2. Mr. Van Dyke's Opinions are Reliable and Will Provide Valuable Assistance to the Court

The Court should reject Respondent's contention that the opinions of Complaint Counsel's expert Mr. James Van Dyke are not sufficiently connected to the facts of this case. Resp't's Post-Trial Brief at 80-82. Rule 702 requires that expert testimony must fit the issues in the case, meaning it "must be relevant for the purposes of the case and must assist the trier of fact." *Schneider ex rel. Estate of Schneider v. Fried*, 320 F.3d 396, 404 (3d Cir. 2003); *see also* Fed. R. Evid. 702). There is no question that Mr. Van Dyke's opinions meet this threshold. As set forth below, Mr. Van Dyke is an expert on identity theft, and his opinions on the issue of likely, quantifiable consumer harm through identity theft are based on a reliable methodology

applied to the facts of this case. Mr. Van Dyke's opinions will be helpful to the Court in determining the likelihood of consumer harm resulting from LabMD's inadequate data security practices.

i. Mr. Van Dyke Properly Analyzed the Likelihood of Consumer Harm as Applied to the Facts of This Case

Mr. Van Dyke, the founder and president of Javelin Strategy & Research (Javelin), is a leader in independent research on customer-related security, fraud, payments, and electronic financial services. CCFF ¶¶ 22-23. Based on a thorough review of the facts of this case and his experience and professional qualifications, Mr. Van Dyke offered opinions assessing the risk of injury to consumers whose personally identifiable information (PII) has been disclosed by LabMD without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure. CCFF ¶¶ 24-25. In its brief, LabMD incorrectly asserts that Mr. Van Dyke's analysis is "wholly disconnected from the facts of the case" and that Mr. Van Dyke allegedly admitted he never considered the specific facts at issue here.[63] Resp't's Post-Trial Brief at 80. LabMD's arguments are without merit.

Contrary to LabMD's assertions, Mr. Van Dyke's opinions are based on a reliable methodology that he applied to the facts of this case.[64] Indeed, Mr. Van Dyke testified at length regarding the methodology used in forming his opinions, demonstrating that it is reliable and will assist the Court. CCFF ¶¶ 30, 36; Van Dyke, Tr. 601-611, 617-632. Among the many steps

---

[63] LabMD claims that Mr. Van Dyke made an "open admission that he never considered any of the specific facts of the case;" that allegation is not supported by the two pages of the 2014 Identity Fraud report that LabMD relies on. Resp't's Post-Trial Brief at 80 (citing CX0741 (Van Dyke Report) at 72-73).

[64] Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony.

taken in forming his opinions, Mr. Van Dyke looked at the portion of people who had their Social Security Number (SSN) exposed in Javelin's nationally representative Identity (ID) Fraud Survey conducted in 2013. CCFF ¶ 28.[65] Mr. Van Dyke then compared those figures to the total quantity of LabMD's consumers who had their personally identifiable information, including their SSNs and other elements of Personal Information, exposed. CCFF ¶ 28. In doing so, Mr. Van Dyke was able to quantify both the incidence rate and financial impact of identity fraud that was likely to occur as a direct result of exposure of consumer personally identifiable information (PII) by LabMD. CCFF ¶¶ 1736-1739; Van Dyke, Tr. 601-602. The calculations of the incidence rates as applied to the LabMD-specific disclosures are supplied in Mr. Van Dyke's report and are supported by the accompanying spreadsheets. CX0741 (Van Dyke Report) at 97-102. There is simply no merit to LabMD's unsupported claim that Mr. Van Dyke did not consider the facts of this case.

LabMD next argues that Mr. Van Dyke's analysis did not account for different types of data breaches by different actors, and contends these factors may be relevant to consumer injury. Resp't's Post-Trial Brief at 80. Respondent presented no evidence in support of this theory, and its suggestion in this regard is misleading. As Mr. Van Dyke has explained, based on the survey data he has fielded for 10 years, the exact profile of a recipient of unauthorized information is not important for predicting in a statistically significant manner what is likely to occur next. Van Dyke, Tr. 734. Rather, the single overriding factor for the purpose of calculating fraud impacts is whether the individual who had access was authorized to receive the information. Van Dyke,

[65] Javelin's nationally representative Identity (ID) Fraud Survey is fielded annually. CCFF ¶ 27. The 2014 Identity Fraud report is based on the 2013 Javelin Identity Fraud Survey. CCFF ¶ 27.

Tr. 734. Moreover, Mr. Van Dyke testified that he specifically considered whether the Day Sheets were "in the hands of unauthorized parties" and he was aware that those documents "were found in the possession of individuals that have pleaded no contest to identity theft." Van Dyke, Tr. 645-646; *see also* CCFF ¶¶ 1413-1458. LabMD has not addressed any of this testimony. Nor has LabMD shown that incorporating the additional factors it cites, such as the type of breach or the profile of the unauthorized recipient, would alter Mr. Van Dyke's analysis.

LabMD further criticizes Mr. Van Dyke's methodology on grounds relating to timing of injury. As to the 1718 File, Complaint Counsel made clear on June 24, 2015 that it would not rely on Mr. Van Dyke's injury calculations applying the 2014 Identity Fraud report to the 1718 File. *See* Compl. Counsel's Opp. to Resp't's Mot. to Admit Selected Exhibits at 10-11 n.11 (June 24, 2015).

As to the Day Sheets, Mr. Van Dyke selected survey data from 2013 because consumers were notified of the unauthorized disclosure of the Day Sheets in March 2013. CCFF ¶ 36. Mr. Van Dyke has explained that his analysis is primarily based on Javelin's nationally-representative Identity Fraud Survey, which is fielded annually. CX0741 (Van Dyke Report) at 4. This survey determined the percentage of survey participants notified that their information was compromised in a data breach in the last 12 months, and the percentage of survey participants who reported becoming victims of identity fraud in the last 12 months. CX0741 (Van Dyke Report) at 6, 8. Specifically, the notification in March 2013 for the Day Sheets "matched up to the period, the twelve-month period" from November 2012 to October 2013 when survey data was collected. Van Dyke, Tr. 603-604. As a result, the data Mr. Van Dyke relied upon in conducting his analysis is most closely aligned with the circumstances of the Day Sheet disclosure.

Similarly unsupported is Respondent's contention that Mr. Van Dyke should have provided different calculations of harm based on how long the unauthorized disclosure was available. Resp't's Post-Trial Brief at 81. There is nothing to suggest any additional calculations of harm to consumers were necessary or appropriate. Rather, as Mr. Van Dyke testified, the twelve-month period of time covered in the 2013 Javelin Identity Fraud Survey properly sets forth a snapshot that captures what frauds breach victims experienced. Van Dyke, Tr. 740. Based on that data, Mr. Van Dyke provided reliable opinions quantifying the amount of likely out-of-pocket costs and hours spent to resolve fraud likely to occur within a twelve month period for individuals impacted by unauthorized disclosure of the Day Sheets. Van Dyke, Tr. 691-692.

Finally, the Court should reject LabMD's suggestion that because there is no evidence of actual consumer injury Mr. Van Dyke's opinions are unreliable. Resp't's Post-Trial Brief at 81-82. As Mr. Van Dyke explained, his approach for forming opinions in this case was based on ten years of experience conducting a methodologically rigorous survey of over 5,000 people with the assistance of statistical experts. Van Dyke, Tr. 730-731. His opinions quantify likely harm to consumers resulting from LabMD's unauthorized disclosures within a twelve-month period. Van Dyke, Tr. 687, 691-692. Mr. Van Dyke further explained that medical identity fraud may be a lifelong threat for consumers affected by LabMD's unauthorized disclosures, such that consumer injury may occur well into the future. CX0741 (Van Dyke Report) at 14. Given that the types of personally identifiable information (PII) that rarely change can be used fraudulently for extended periods of time once compromised, placing consumers at risk of injury indefinitely, CCFF ¶ 1566, Mr. Van Dyke's opinion of likely harm is conservative. For all of these reasons, Mr. Van Dyke's opinions will assist the Court and should be considered.

3. Mr. Kam's Opinions are Reliable and Will Provide Valuable Assistance to the Court

The Court should reject LabMD's contention that the opinions of Complaint Counsel's expert Mr. Kam should be accorded little or no weight. Resp't's Post-Trial Brief at 82-86. Rather than conduct its own study, LabMD criticizes Mr. Kam's opinions on several grounds, including that: (i) the methodology was not "peer reviewed," published, or used by other industry experts; (ii) the analysis was not sufficiently connected to the facts of this case; (iii) actual consumer injury emanating from the 1718 File impacts the reliability of the opinions; and (iv) certain alleged harms are not cognizable under Section 5 of the FTC Act.[66] As set forth below, none of LabMD's arguments withstand scrutiny. Mr. Kam possesses the necessary experience and specialized knowledge to provide expert testimony on the risk of consumer injury—particularly as it relates to medical identity theft—and the opinions Complaint Counsel relies on are reliable, clearly admissible under *Daubert*, and entitled to the Court's full consideration.

---

[66] Resp't's Post-Trial Brief at 82-86. Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. In addition, Complaint Counsel's proposed findings of fact cite to CX0451, Mr. Wilmer's spreadsheet identifying consumers included in the Sacramento incident whose Social Security numbers are being used by multiple persons, only to preserve its rights with respect to admission of the document.

Complaint Counsel has not marked as nonpublic its reference to CX0451 (*in camera*) because the (1) the exhibit has been granted *in camera* status due to the inclusion of Sensitive Personal Information as defined in Rule 3.45(b) and (2) the citation is to the existence or nature of the exhibit, rather than to specific Sensitive Personal Information contained therein

i. Mr. Kam's Methodology For Assessing Risk of Injury to Consumers is Reliable[67]

Mr. Kam, a Certified Information Privacy Professional (CIPP/US), leads and participates in several cross-industry data privacy groups, regularly publishes relevant articles in the field, and works on development of policy and solutions to address the protection of health information and personally identifiable information, as well as remediating privacy incidents, identity theft, and medical identity theft. CCFF ¶ 38. Mr. Kam is president and co-founder of ID Experts, a company specializing in data breach response and identity theft restoration. CCFF ¶ 38. Based on a thorough literature review, documents Mr. Kam received from Complaint Counsel, and his professional experience and qualifications, Mr. Kam offered opinions assessing the risk of injury to consumers caused by the unauthorized disclosure of consumers' sensitive Personal Information. CCFF ¶¶ 39-41.

In its brief, LabMD wrongly asserts that Mr. Kam's methodology is unreliable because it is not "peer reviewed," published, or used by other industry experts. Resp't's Post-Trial Brief at 82. It is well-settled that the *Daubert* factors, including whether a theory or technique "can be (and has been) tested" or "has been subjected to peer review and publication" or its "general acceptance," are not the only means to assess the reliability of an expert's methodology; courts may consider other factors relevant to the expert's field. *See Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. at 593-595 ("The inquiry envisioned by Rule 702 is, we emphasize, a flexible one."); *Kumho Tire Co., Ltd.*, 526 U.S. at 150-151 (*Daubert* factors are "meant to be helpful, not definitive."). Because there are many different types of experts and many different types of

[67] Complaint Counsel's subheading structure differs from Respondent's in this section. Complaint Counsel's Section Argument, II.B.3.i responds to Respondent's Sections Argument,

expertise, the relevant reliability concerns may focus upon the expert's personal knowledge or experience. *See Kumho*, 526 U.S. at 150; Fed. R. Evid. 702 advisory committee's note; *Pension Comm. of the Univ. of Montreal Pension Plan*, 691 F. Supp. 2d at 473.

Mr. Kam's analysis of the risk of consumer injury is based on his extensive experience working in the field of identity theft victim restoration, as well as his knowledge of relevant literature concerning identity theft, medical identity theft, and consumer privacy. CX0742 (Kam Report) at 3-5, 10-11, 13-15, 33-36; RX522 (Kam, Dep. at 36-37, 44-46, 72-73). In analyzing the harm of LabMD's unauthorized disclosures, Mr. Kam considered the nature and extent of the sensitive Personal Information involved in an unauthorized disclosure, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the protected health information or to whom the disclosure was made; whether the sensitive Personal Information was actually acquired or viewed; and the extent to which the risk to the protected health information has been mitigated. CX0742 (Kam Report) at 17-18; CCFF ¶ 43. Mr. Kam derived this framework from his work with clients, which he outlined throughout the report, as well as his literature review. CX0742 (Kam Report) at 10, 13-15, 33-36; RX522 (Kam, Dep. at 36-37, 44-46, 72-73).

Mr. Kam's analysis is a fact-dependent inquiry, and the application of his analysis to this case is informed by his work experience. RX522 (Kam, Dep. at 72-73). Mr. Kam's judgment in assessing how each unauthorized disclosure or security failure creates particular risks is informed by years of experience in responding to unauthorized disclosures. CX0742 (Kam Report) at 3, 13-14. Mr. Kam explains in detail how he applied his experience to the facts of the

---

II.B.3.i, Resp't's Post-Trial Brief at 82-83 and Argument, II.B.3.ii, Resp't's Post-Trial Brief at 83.

LabMD unauthorized disclosures and security failures, how his experience led to his opinions on the likelihood of harm resulting from LabMD's disclosures of sensitive personal information, and why his experience provides sufficient bases for those opinions. (CX0742 (Kam Report) at 10-12, 18-19, 21-23).

ii. Mr. Kam's Analysis of the Day Sheets Is Sufficiently Applied to the Facts of This Case

Contrary to LabMD's assertions, Mr. Kam's analysis is sufficiently connected to the facts of this case.[68] A qualified expert may offer testimony when the testimony is based on sufficient facts, and the expert reliably applies principles and methods to the facts of the case. Fed. R. Evid. 702; *Schneider*, 320 F.3d at 404. Mr. Kam reliably applied his expertise to the facts of this case and his testimony should therefore be considered by the Court.

Mr. Kam's opinion regarding harm likely to result from disclosure of the Day Sheets is specific to the information in those documents. CX0742 (Kam Report) at 23. Mr. Kam considered the Day Sheets, investigation, pleas entered by the identity thieves,[69] and offered his opinion on the harm that may result based on his knowledge of unauthorized disclosures and identity crimes. CX0742 (Kam Report) at 21-23; RX522 (Kam, Dep. at 154-155).

---

[68] As noted above, Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. In addition, Complaint Counsel's proposed findings of fact cite to CX451, Mr. Wilmer's spreadsheet identifying consumers included in the Sacramento incident whose Social Security numbers are being used by multiple persons, only to preserve its rights with respect to admission of the document.

[69] While Mr. Kam relied on the incorrect assumption that the persons who had possession of the Day Sheets and copied checks had prior convictions for identity theft, they both pleaded *nolo contendere* to felony charges of identity theft in connection with the Sacramento incident. CCFF ¶¶ 1455-1457.

iii. Mr. Kam's Analysis of the 1718 File Is Sufficiently Applied to the Facts of This Case

Mr. Kam reviewed numerous documents provided to him by Complaint Counsel and applied his analysis to the facts of this case, including the 1718 File. CX0742 (Kam Report) at 6-8. Mr. Kam's analysis of harm from unauthorized disclosure of the 1718 File also considered the volume and sensitivity of the information contained within it. CX0742 (Kam Report) at 18. His opinion of the reputational harm that may result from the unauthorized disclosure of the 1718 File is rooted in a detailed analysis of the disclosed CPT codes. CX0742 (Kam Report) at 6, 18, 21, 39-48. Mr. Kam's calculation of the financial harms in out-of-pocket costs and other injuries consumers will likely suffer due to unauthorized disclosure of the 1718 File is also based on the specific types and amount of data exposed. CX0742 (Kam Report) at 19-20. Mr. Kam applied the findings of the Ponemon Institute's 2013 Survey on Medical Identity Theft to aid his analysis of the likely risk of harm faced by the 9,300 consumers whose information was disclosed by LabMD. CX0742 (Kam Report) at 19; RX522 (Kam, Dep. at 106).

Mr. Kam's opinions are reliable notwithstanding LabMD's claim that evidence of actual consumer injury is lacking. Resp't's Post-Trial Brief at 84. Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury. CCCL ¶ 25. The inquiry turns on whether any potential or actual unauthorized disclosure of Personal Information held by a company due to unreasonable data security practices caused or is likely to cause consumer harm. CCCL ¶ 25.

LabMD's argument also fails because Mr. Kam has explained at length in his report and at trial that consumers may be vulnerable to identity theft harms for a long period of time. *See* CCFF §§ 8.1.1.5.5 (Consumers May be Vulnerable to Identity Theft Harms For a Long Period of Time) *et seq.* (¶¶ 1566-1567); 8.1.1.5.5.1 (SSNs are Especially Valuable Pieces of Information to

Identity Theives for a Long Period of Time) *et seq.* (¶¶ 1570-1575); 8.1.1.6.1 (Identity Theft Harms Can Take Months to Years to Identify) *et seq.* (¶¶ 1578-1580); 8.1.1.6.2 (Identity Theft Harms are Difficult to Remediate Once Identified) *et seq.* (¶¶ 1583-1584). Contrary to LabMD's assertions, Mr. Kam's analysis does not depend on the presence or absence of actual injury by a date certain.

iv. Mr. Kam Properly Opined on the Types of Harms to Consumers Stemming From Unauthorized Disclosure of the 1718 File

Mr. Kam properly opined on harms to consumers that support a finding of substantial injury under Section 5, including reputational and other harms stemming from the unauthorized disclosure of the 1718 File. *See* CCFF §§ 8.3.4.1.1 (Unauthorized Disclosure of CPT Codes Revealing Sensitive Conditions is Likely to Cause Harm) *et seq.* (¶¶ 1684-1692); 8.3.4.1.2 (There is a Significant Risk of Consumer Reputational Harm Due to the Unauthorized Disclosure of the CPT Codes) *et seq.* (¶¶ 1695-1697); 8.3.4.1.3 (Reputational Harm to Consumers May be Ongoing Because Once Health Information is Disclosed, it is Impossible to Restore a Consumer's Privacy) *et seq.* (¶¶ 1700-1701); 8.3.4.2 (Consumers Did Not Receive Notice of the Unauthorized Disclosure of the 1718 File) *et seq.* (¶¶ 1704-1705); 8.3.4.3 (With No Notification of Unauthorized Disclosure, No Mitigation of Harm is Possible) *et seq.* (¶¶ 1708-1711); CCCL § 1.3.1.2 (Substantial Injury) *et seq.* (¶¶ 29-40).

LabMD's contention that reputational harm does not support a finding of substantial injury is unfounded. It is well-settled that the entirety of harms likely to be caused by an unfair act or practice need not be monetarily quantifiable. *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988) (affirming Commission grant of summary judgment where injury included in part "intangible loss" relating to certainty of contract terms). CCCL ¶ 34. Indeed,

loss of privacy can result in a "host of emotional harms that are substantial and real and cannot be fairly classified as either trivial or speculative." *FTC v Accusearch, Inc.*, 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007) (obtaining and selling consumers' confidential phone call records is an unfair practice under Section 5). LabMD's data security failures are likely to cause consumers the loss of privacy, in addition to the health and safety risks associated with medical identity theft. These harms are not "subjective" or "not cognizable," as LabMD claims, and it has failed to show otherwise. Resp't's Post-Trial Brief at 85; *see* CCCL ¶¶ 29-40.

C. Complaint Counsel Has Proven the Elements of Section 5(n)

Section 5's prohibition of unfair acts or practices does not violate Respondent's due process rights, as discussed more fully below.[70]

1. Section 5 Gives Fair Notice of Its Proscriptions

The unfairness definition in the FTC Act, 15 U.S.C. § 45(n), "is sufficient to give fair notice of what conduct is prohibited." Comm'n Order Denying Resp't's Mot. to Dismiss at 16 (Jan. 16, 2014); *see also supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-68. That prohibition applies across industries. *See infra* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41. The Commission is not required to promulgate rules relating to data security before enforcing Section

[70] Respondent includes in this subsection conclusory statements restating arguments that appear elsewhere in its brief. Complaint Counsel addressed Respondent's claim that proof of recurrence is an element of Section 5(n), Resp't's Post-Trial Brief at 86, *supra* Burden of Proof, § I (Complaint Counsel's Burden of Proof is Defined by Section 5), at 42-43. Complaint Counsel addressed Respondent's claim that, contrary to Section 5's requirement that an act or practice be likely to cause harm, proof of data breach is required, Resp't's Post-Trial Brief at 86, *supra* Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 96.

5 of the FTC Act in the data security context. Comm'n Order Denying Resp't's Mot. to Dismiss at 14-15 (Jan. 16, 2014); *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d at 617-619, *aff'd*, No. 14-3514, WL 4998121, (3d Cir. Aug. 24, 2015) (finding that precedent does not "require[] the FTC to formally publish a regulation before bringing an enforcement action under Section 5's unfairness prong"); *POM Wonderful LLC v. FTC*, 777 F.3d 478, 497 (D.C. Cir. 2015) (affirming that the Commission "validly proceeded by adjudication" and is not required to engage in rulemaking even where an administration decision may "affect agency policy and have general prospective application" (citations omitted)).

The test under Section 5 unfairness in the data security context, as the Commission recently expressed it, is reasonableness:[71] "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities." Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf. As with the application of the reasonableness standard of care in any other circumstance, what constitutes reasonable data security practices for a company that maintains consumers' sensitive Personal Information will vary depending on the circumstances. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) ("[T]he proscriptions in [Section] 5 are flexible, 'to be defined with

[71] While Complaint Counsel drew this test from the Commission's guidance, as noted in the Commission Order Denying LabMD's Motion for Summary Decision, "the Commission is not bound by Complaint Counsel's arguments or characterizations" regarding data security standards. Comm'n Order Denying Resp't's Mot. for Summary Decision at 7 n.12 (May 19, 2014).

particularity by the myriad of cases from the field of business.'") (internal citations omitted)); *Brock v. Teamsters Local Union No. 863*, 113 F.R.D. 32, 34 (D.N.J. 1986) (reasonableness under prudent man standard "tried on the individual facts of [the] case" in light of standards developed in case law); *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3-4 (D. Nev. Sept. 9, 2013) (applying "reasonable and prudent person" standard in negligence case for failure to safeguard electronically held data). Reasonableness turns on the amount and sensitivity of the information the company handles (going to the magnitude of injury from unauthorized access to information) and the nature and scope of the firm's activities (going to the structure of the firm's network, how the network operates, the types of security vulnerabilities and risks it faces, and feasible protections). *See* Comm'n Statement Marking 50th Data Sec. Settlement; *Cf. FTC v Accusearch, Inc.*, 2007 WL 4356786, at *7 (D. Wyo. Sept. 28, 2007) (defendants "can reasonably be expected to know" the legal environment in which they operate).

2. Dr. Hill's Report is not Dependent on Testimony from Mr. Boback or Tiversa

Complaint Counsel's precomplaint investigation is irrelevant to the disposition of this proceeding. *See supra* Facts, § I.B.3 (Third Party Witness Tiversa), at 9-10. The Commission initiates investigations based on a variety of sources. *Cf. Osborne v. Grussing*, 477 F.3d 1002, 1007 (8th Cir. 2007) (agencies routinely act on the basis of information provided by private parties with a personal interest, and "[w]hen such a complaint results in enforcement action, we do not impute the complainant's ulterior motive to the government enforcers"). Moreover, there is no dispute that the 1718 File was available on a P2P network and was downloaded from the P2P network in February 2008. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 4; Wallace, Tr. 1393-95. Dr. Hill's opinion on other aspects of LabMD's data security are based on her examination of the evidence and not based on evidence from either Mr. Boback or Tiversa. *See*

supra Argument, § II.B.1.ii (Dr. Hill Properly Analyzed Data Security Standards as Applied to LabMD and Her Opinions Fit the Facts of This Case), at 106-09. Dr. Hill's opinions are relevant and will assist the Court to understand the evidence or to determine a fact in issue. Fed. R. Evid. 702(a); *see supra* Argument, § II.B.1.ii (Dr. Hill Properly Analyzed Data Security Standards as Applied to LabMD and Her Opinions Fit the Facts of This Case), at 106-09.

3. Complaint Counsel Has Proven that LabMD's Unfair Practices Caused or Likely Caused Substantial Injury to Consumers That Was Not Outweighed by Countervailing Benefits to Consumers or Competition

Respondent's arguments relating to Complaint Counsel's burden of proof to establish that LabMD caused or likely caused injury to consumers, Resp't's Post-Trial Brief at 88-89, have been previously addressed.

Complaint Counsel need not, as Respondent claims, Resp't's Post-Trial Brief at 88-89, identify a complaining witness nor prove injury to any specific consumer; demonstrate that the 1718 File and Sacramento Incidents, [72] in which Personal Information maintained by LabMD was found outside its network and files, were "actual" breaches; or present evidence on any breach at all. *Supra* Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 96.

Complaint Counsel has addressed Respondent's attempt to add another element to its Section 5(n) burden of proof, recurrence, Resp't's Post-Trial Brief at 88, *supra*. Burden of Proof, § I (Complaint Counsel's Burden of Proof is Defined by Section 5), at 42-43.

---

[72] Complaint Counsel does not dispute that LabMD provided notice to the individuals in the Day Sheets and copied checks in the Sacramento incident. *See* Resp't's Brief at 88-89.

Complaint Counsel has proven that the consumer injury LabMD caused or likely caused through its unfair conduct was not reasonably avoidable by the consumers, Argument, § II.A.3 (Consumers Could Not Reasonably Avoid Injury Caused or Likely Caused by LabMD), at 99-100, contrary to Respondent's claims. Resp't's Post-Trial Brief at 88.

Respondent's remaining argument is that Complaint Counsel failed to prove that the injury, or likely injury, LabMD's unfair conduct caused was "not outweighed by countervailing benefits to consumers or to competition," 15 U.S.C. § 45(n). Resp't's Post-Trial Brief at 88. LabMD's unreasonable data security practices were not offset by countervailing benefits to consumers or competition.[73] Countervailing benefits are determined based on the specific practice at issue in a complaint, in this instance unreasonable data security, not the overall operation of a business. *FTC v. Accusearch, Inc*., 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009) ("While there may be countervailing benefits to some of the information and services provided by 'data brokers' such as *Abika.com*, there are no countervailing benefits to consumers or competition derived from the specific practice of illicitly obtaining and selling confidential consumer phone records." (emphasis original)); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (upholding Commission finding of no countervailing benefits because an increase in fees "was not accompanied" by an increased level or quality of service); *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 2 (Jan. 15, 2014) (reiterating that countervailing benefit determination is made by "compar[ing] that harm to any benefits from that particular practice"). In the cybersecurity

[73] Respondent once again argues, in the context of Section 5(n)'s cost-benefit analysis, that the standard for the medical industry should differ from Section 5's usual application. This argument is wrong. *Infra* Argument, § II.C.5.d (Section 5's Unfairness Standard Applies Across Industries), at 139-41.

context, the cost-benefit analysis "considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." *FTC. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121, at *13(3d Cir. Aug. 24, 2015).

LabMD holds the sensitive Personal Information of 750,000 consumers, and provided *no* services to over 100,000 of them. CCFF ¶¶ 12, 71, 78-79. "'[W]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition,'" the countervailing benefits prong of the unfairness test is "easily satisfied." *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (quoting *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000)). The cost to correct many of LabMD's security failings was low, in many cases requiring only employee time to implement reasonable data security practices. *See generally* CCFF § 5, ¶¶ 1113-1185 (LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low Cost Measures). The low cost indicates that correcting these security failures would impose little or no additional costs to consumers, and thus little or no benefit would accrue from not correcting the security failures. Where an unfair practice does not provide any advantages in the marketplace, any benefits that may accrue are "small." *Neovi, Inc.*, 598 F. Supp. 2d at 1116. Indeed, LabMD has not identified any alleged "additional burdens to . . . doctors and their patients" its practice of reasonable security would have imposed. Resp't's Post-Trial Brief at 88.

Furthermore, the countervailing benefit analysis is a "tradeoff" that must be "sufficient to offset the human injuries involved." *Int'l Harvester Co.*, Docket No. 9147, 104 F.T.C. 949, 1065, 1984 WL 565290, at *90 (1984). As the potential harm from unauthorized disclosure of

consumer data held by a company increases, as is the case with the Personal Information held by LabMD, *see* CCFF ¶¶ 1667-1671, 1714-1719 (the type of information LabMD held is valuable to identity thieves), the offsetting benefits from not correcting its security failures must be correspondingly higher to justify inaction. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) ("[T]he proscriptions in [Section] 5 are flexible, 'to be defined with particularity by the myriad of cases from the field of business.'" (internal citations omitted)); Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf ("[A] company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities"). Here, the human cost of subjecting consumers to a likelihood of harm in the form of identity theft and identity fraud is high, and the burden of adopting low cost reasonable data security measures is low. *See generally* CCFF § 8, CCFF ¶¶ 1472-1798 (LabMD's Data Security Practices Caused or a Likely to Cause Substantial Injury to Consumers That is Not Reasonably Avoidable by the Consumers Themselves and Are Not Outweighed by Countervailing Benefits to Consumers or Competition); CCFF § 5, CCFF ¶¶ 1113-1185 (LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low Cost Measures).

4. LabMD Had Control Over and Was Responsible For Its Own Unreasonable Data Security

LabMD's argument that, as a matter of law, it should prevail if it reasonably relied on IT experts to design and implement its IT systems, is without merit. Resp't's Post-Trial Brief at 43, 68, 96 n.18. As an initial matter, it is unclear from LabMD's post-trial brief whether LabMD

is referring to its reliance on *external or internal* IT "experts" (emphasis added). Either way, its argument fails.

To the extent that LabMD is referring to its use of external IT providers, LabMD's assertion fails because from it did not rely on outside experts for most of the relevant time period. From at least 2006, LabMD managed its network using in-house IT employees and did not rely on outside service providers for its network security. CCFF ¶¶ 173, 175, 178, 182-183, 185-186, 188, 190; *supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 5-8. Although LabMD engaged APT, as described above, it did not engage that company to provide security services; rather, APT was supposed to set up LabMD's network and troubleshoot problems, such as those involving Internet speed and connectivity. CCFF ¶ 185; *see also supra* Facts, § I.A.1 (LabMD Did Not Seek Expert Advice on Data Security), at 6-7.

To the extent that LabMD is referring to its use of internal IT staff, it defies logic and well-settled law that LabMD should be shielded from liability based on conduct of its own employees. *See Meyer v. Holley*, 537 U.S. 280, 285 (2003) ("It is well established that traditional vicarious liability rules ordinarily make principals or employers vicariously liable for acts of their agents or employees in the scope of their authority or employment." (citations omitted)).

Second, in support of its argument, LabMD cites to two highly distinguishable cases involving the Occupational Safety and Health Act (OSHA). Resp't's Post-Trial Brief at 43, 96 (citing *Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1083 (D.C. Cir. 2007) and *R.P. Carbone Constr. Co v. OSHRC*, 166 F.3d 815, 819-20 (6th Cir. 1998)). Complaint Counsel has addressed Respondent's claim that OSHA somehow modifies Section 5's burden of proof *supra*, Argument, § II.A.4 (Section 5 is Not Modified by OSHA), at 100-01. Even if these cases were

applicable to LabMD's utilization of certain IT contractors in limited circumstances, LabMD mischaracterizes them. They do not hold, as LabMD asserts, that "reasonable reliance on subcontractors who were experts relieves contractor from liability." Resp't's Post-trial Brief at 96 n.18.

Rather, the Courts acknowledge that a primary contractor's reliance on a specialist to prevent hazards outside the contractor's area of knowledge *and over which the primary contractor has little to no control* may in certain circumstances negate the primary contractor's liability under OSHA. *See Fabi Constr. Co.*, 508 F.3d at 1083 (finding that primary contractor was not entitled to rely on subcontractor to relieve itself of OSHA liability following parking garage collapse); *R.P. Carbone Constr. Co.*, 166 F.3d at 818-820 (affirming $1,500 citation for OSHA violation against general contractor for failing to comply with worker-safety requirements involving fall protection and prevention measures). Here, LabMD's own Findings of Fact establish that LabMD shared IT functions with APT and did not relinquish control to APT. RFF ¶ 157. Further, to the extent that LabMD's argument is premised on its own internal IT staff, LabMD has not demonstrated that it lacked control over its own IT staff, but instead has argued that Mr. Boyle and Mr. Hyer supervised the staff closely. Resp't's Post-Trial Brief at 30 (Boyle), 33 (Hyer).

5. Complaint Counsel Has Proven that LabMD Had Unreasonable Security

Respondent includes a final scattershot volley reiterating many of its previous arguments.[74] Resp't's Post-Trial Brief at 90-97. Complaint Counsel has already addressed Mr.

[74] Respondent acknowledges that Section 5's reasonableness test is the law of the case, Resp't's Post-Trial Brief at 92. Given that concession, Complaint Counsel does not add to its prior discussion of this standard.

Fisk's unfounded opinion that LabMD maintained reasonable data security, Resp't's Post-Trial Brief at 90. *Supra* Facts, § II.B (Mr. Fisk's Testimony Does Not Establish That LabMD Had Reasonable Data Security), at 34-37.

Respondent attempts yet again to amend Section 5, arguing that Complaint Counsel must prove "there was an actual data breach, *and* if one occurred, that consumers suffer substantial injury *and* that LabMD's data security practices are unreasonable." Resp't's Post-Trial Brief at 92. Respondent's strenuous insistence does not change the statutory elements, a prerogative preserved for Congress, as discussed *supra*. Argument, § II.A.2 (Complaint Counsel Has Met Its Burden to Prove LabMD's Practices Caused or Are Likely to Cause Substantial Injury), at 95-98.

Respondent argues, in various terms, that HIPAA preempts Section 5, that Complaint Counsel must prove Respondent violated HIPAA, and that Section 5 does not apply to LabMD. Resp't's Post-Trial Brief at 92-93, 95-96. Complaint Counsel demonstrated that HIPAA does not preempt the FTC Act *supra*. Argument, § I.B (HIPAA Does Not Preempt Section 5), at 60-62.

Complaint Counsel addressed Respondent's claim that OSHA modified the Section 5 unfairness standards, Resp't's Post-Trial Brief at 94, *supra*. Argument, § II.A.4 (Section 5 is Not Modified by OSHA), at 100-01.

Complaint Counsel addresses the remainder of Respondent's arguments below.

a. The Commission Has Provided Warnings on the Dangers Posed by Use of P2P Networks Since 2003[75]

Respondent's claim that the FTC did not issue any warnings until February 2010, Resp't's Post-Trial Brief at 91-92, is in direct opposition to overwhelming and uncontroverted evidence. The Commission began issuing warnings about the dangers of P2P file sharing in 2003. *See* CCFF ¶¶ 1338-1351; CX0770 (FTC CONSUMER ALERT: FILE-SHARING: A FAIR SHARE? MAYBE NOT (2003)) at 2 (2003 publication warning that use of P2P software may "unknowingly allow others to copy private files you never intended to share."); CX0771 (Press Release, Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure at 2 (Apr. 2, 2004)) (2004 publication warning that use of P2P software could "lead to viruses, as well as a competitor's ability to read the files on your computer."); CX0773 (*Hearing on Online Pornography: Closing the Door on Pervasive Smut: Before the H. Subcomm. on Commerce, Trade, and Consumer Prot., H. Comm. On Energy and Commerce),* 108th Cong. (May 6, 2004) (statement of J. Howard Beales, Dir., Bureau of Consumer Prot., FTC: at 6-7 (discussing "the security risks of improperly configuring P2P file-sharing software, including the risk that sensitive personal files inadvertently may be disclosed")). Respondent presents no argument that explains why it ignores the Commission's many warnings provided to consumers, businesses, and Congress before 2010 that are in evidence in this proceeding.[76]

---

[75] Respondent's post-trial brief does not contain subheadings in this section; Complaint Counsel has added them for the ease of the reader.

[76]Respondent's apparently rhetorical questions in footnote 17 of its brief are based on a false premise. Resp't's Post-Trial Brief at 91 n.17. Respondent attempts to manufacture implications from its supposed "fact" that the FTC did not warn of the dangers of P2P until January 2010

Respondent's statement that the "FTC . . . had been *partnering* for years with LimeWire and other P2P software providers," Resp't's Post-Trial Brief at 90 (emphasis original), is made without any explanation or any support in the record. Respondent's citation page 26 of the 2005 Staff Report on P2P technology does not shed any light on what manner of "partnership" it is alleging. *See* CX0777 (FED. TRADE COMM. STAFF: PEER-TO-PEER FILE-SHARING TECHNOLOGY: CONSUMER PROTECTION AND COMPETITION ISSUES (2005)). If Respondent intends to suggest that the fact that the report "encourages the P2P file-sharing industry to continue its efforts to decrease these risks through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education," *id.* at 32 constitutes "partnership" with LimeWire, then it utterly fail to provide any support for such a leap of logic and linguistics.[77]

b. **Respondent's Internal Investigation of its Sharing of the 1718 File on a P2P Network Does Not Demonstrate It Had Reasonable Data Security**

Complaint Counsel has introduced overwhelming evidence of LabMD's unreasonable LabMD's data security practices. For instance, LabMD did not enforce its policy restricting downloads from the Internet; until at least 2010, it gave most employees administrative access to their computers, which allowed them to install programs as well as to change security settings. CCFF ¶¶ 1055-1059. As a result, LimeWire was downloaded and installed to the computer used by the billing manager in or about 2005, and was used on that computer until May 2008, when LabMD was informed that it had shared the 1718 File on the P2P network. CCFF ¶¶ 1061,

---

(rather than February 2010, as it stated in the text). Because the FTC has been issuing warnings about the dangers of P2P since 2003, these questions need not be answered.

[77] Respondent also cites to a letter with a URL that is no longer active and that Respondent has not moved for admission. This violates the Court's Order on Post-Trial Briefs because the evidence cited is not in the record. Order on Post-Trial Briefs at 2 (July 16, 2015).

1365; CX 0730 (Simmons, Dep. at 14-15). LabMD's internal investigation of this incident after its Billing Manager had been sharing the entire My Documents folder of her computer on a P2P network for up to three years, CCFF ¶ 1368, does not demonstrate that it had reasonable security.[78]

Respondent also claims that it "continually updated its Employee Handbook . . . to reflect reasonable and adequate data security policies under HIPAA/HITECH." Resp't's Post-Trial Brief at 92. LabMD's Employee Handbook lacked policies relating to data security. CCFF ¶¶ 422-426. The Handbook claims that LabMD took "specific measures to ensure [its] compliance with [HIPAA]." CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6. It does not mention what those measures are; nor does it mention whether the measures relate to privacy (e.g., providing consumers with access to their own data) or security. In addition, no LabMD employee — including LabMD's President and CEO — could describe what mechanisms LabMD implemented to achieve the stated goal of "specific measures" to comply with HIPAA. CX0725-A (Martin, Dep. at 166-67); CX0711 (Dooley, Dep. at 144-46); CX0719 (Hyer, Dep. at 162-63); CX0733 (Boyle, IHT at 248-49); CX0710-A (Daugherty, LabMD Designee, Dep. at 119).

Finally, there is no evidence in the record that LabMD purchased hundreds-of-thousands of dollars of additional IT software and hardware above and beyond other small laboratories, or

---

[78] Among other things, Respondent asserts that the Billing Manager was fired as a result of the incident. The evidence shows that she was fired for poor performance as well as the P2P incident. CX0765 (Resp't's Resps. to Second Set of Discovery) at 11 (Resp. to Interrog. 19); CX0704-A (Boyle, Dep. at 156); CX0736 (Daugherty, IHT at 91). This is further supported by the fact that she was not terminated until two months after the incident, on July 31, 2008. CX0681 (Rosalind Woodson Dates of Employment) at 7.

indeed that it purchased hundreds-of-thousands of dollars of IT software and hardware at all, and Respondent makes this assertion without any reference to the record or factual support in violation of the Court's Order on Post-Trial Briefs. Resp't's Post-Trial Brief at 92. In fact, the evidence shows that LabMD IT employees used low-quality products without full functionality, that LabMD had no established IT budget, and that LabMD IT employees had no discretion to purchase IT equipment, applications, or training. CCFF ¶¶ 1115-1118. And even if LabMD's assertion were true, improperly configured hardware and software that is not updated is vulnerable—and proper configuration is often a low cost measure.[79] Where the cost to correct a failure is low, consumers recognize little to no benefit from the failure. *See supra* Argument, § II.C.3 (Complaint Counsel has Proven that LabMD's Unfair Practices Caused or Likely Caused Substantial Injury to Consumers That Was Not Outweighed by Countervailing Benefits to Consumers or Competition), at 128-31.

With respect to the other known breach of Personal Information maintained by LabMD, the Sacramento Incident, Respondent claims the Day Sheets were stored only in hard copy. Resp't's Post-Trial Brief at 92. However, some of the Day Sheets were scanned and saved to LabMD's computer network as part an archive project by the company. CX0733 (Boyle, IHT at

---

[79] *See, e.g.*, CCFF ¶¶ 1131 (LabMD could have used Windows software firewall included in the operating system it was already running), 1150-1151 (LabMD could have used access controls already embedded in operating systems and applications to control access to information employees did not need to use their jobs), 1152-1154 (LabMD could have purged unneeded Personal Information from its databases through its database application), 1166-1167 (LabMD could have used password management scheme included in its Windows operating system to centrally manage passwords), 1171-1177 (LabMD could have connected to free notification systems to learn of security issues in its software and their solutions and could have applied patches provided at no cost by vendors), 1181 (LabMD could have used standard Windows feature to give employees non-administrative accounts on their computers to prevent them from installing software), 1183 (LabMD could have properly configured its existing firewalls).

37, 46-47). Billing employees also had the option of saving Day Sheets electronically to a computer. CX0714-A ([Fmr. LabMD Empl.]), Dep. at 58-61.

c. **The Commission Properly Proceeded by Adjudication in this Matter**

Respondent rephrases its fair notice claims regarding mandatory Federal Register publication, and also objects to the Commission's decision to proceed by adjudication in this matter. Resp't's Post-Trial Brief at 93-94. Complaint Counsel has previously explained that the Commission is not required to issue a rule or a statement of general policy on data security. *Supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-63 (rule); Argument, § I.C.1.b (Mr. Kaufman's Testimony Did Not Violate the APA), at 68 (general statement of policy).

d. **Section 5's Unfairness Standard Applies Across Industries**

Respondent argues that "medical data security 'reasonableness' under Section 5 as a matter of law is a matter of first impression," Resp't's Post-Trial Brief at 92. But there is no distinct "medical data security 'reasonableness'" under Section 5. Rather, as discussed above, reasonableness is the "touchstone of the Commission's approach to data security," and it applies across industries. Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-68; *supra* Argument, § II.C.1 (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27. Regardless of the industry in which the company operates, the Commission assesses whether a company's data security measures are reasonable and appropriate in light of "the sensitivity and volume of consumer information [a company] holds, the size and complexity of its business, and the cost of

available tools to improve security and reduce vulnerabilities." *See* Comm'n Statement Marking 50th Data Sec. Settlement.

Courts have upheld Section 5's prohibition of "unfair...acts or practices" as a flexible prohibition that applies across industries. *See, e.g., FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972) (applying Section 5 to trading stamps); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (applying Section 5 to televised commercial for shaving cream, and stating that "the proscriptions in [Section] 5 are flexible"); *FTC v. Motion Picture Adver. Serv. Co.*, 344 U.S. 392 (1953) (applying Section 5 to exclusive film-screening agreements); *FTC v. Neovi*, 604 F.3d 1150 (9th Cir. 2010) (applying Section 5 to online check-processing); *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (9th Cir. 2009) (applying Section 5 to online sale of phone records). Congress deliberatively delegated broad power to the FTC under Section 5 to address to address unanticipated practices in a changing economy. *See, e.g., American Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 967-69 (D.C. Cir. 1985).

Respondent argues that because Section 5(n) does not define "unreasonable" data security acts or practices, "there is no statutory basis for a 'reasonableness' determination." Resp't's Post-Trial Brief at 92 (*citing Steadman v. SEC*, 450 U.S. 91, 98 (1981)). *Steadman* is inapposite. In *Steadman*, the petitioner argued that the Administrative Procedure Act's requirement that agency decisions be based on "reliable, probative, and substantial" evidence meant that the SEC must meet a clear-and-convincing standard of proof in its administrative proceedings. *Steadman v. SEC*, 450 U.S. 91, 95-97 (1981). The Court rejected this argument and held that the proper standard of proof was preponderance of the evidence. *Id.* at 102. Steadman has no bearing on the statutory basis for a reasonableness determination. The language of the relevant statute here, Section 5(n), sets forth the requirements for the

Commission to declare an act or practice "unfair." *See* 15 U.S.C. § 45(n) (stating that the Commission "shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."). The unfairness definition in the FTC Act, 15 U.S.C. § 45(n), "is sufficient to give fair notice of what conduct is prohibited." Comm'n Order Denying Resp't's Mot. to Dismiss at 16 (Jan. 16, 2014); *see also FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 619 (D.N.J. 2014), *aff'd*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (rejecting the contention that regulations are the only means to provide fair notice and stating that "Section 5 codifies a three-part test that prescribes whether an act is 'unfair'"); *supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-68; *supra* Argument, § II.C.1 (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27.

D. Entry of the Notice Order is Appropriate and Necessary

For the reasons set forth in its post-trial brief, Complaint Counsel respectfully requests that the Court enter the proposed Notice Order, which was attached to its complaint in compliance with Rule 3.11(b)(3), 16 C.F.R. § 3.11(b)(3). Respondent's arguments that the requested relief is not appropriate all fail for the reasons set forth below.

First, Respondent offers no legal or factual support for its claim that the attachment of the proposed Notice Order to the complaint somehow renders relief inappropriate. Complaint Counsel's complaint is in compliance with Rule § 3.11(b)(3), which requires that "The Commission's complaint shall contain the following: . . . (3) Where practical, a form of order

which the Commission has reason to believe should issue if the facts are found to be as alleged in the complaint." 16 C.F.R. § 3.11(b)(3).

Nor is the relief sought in this proceeding punitive; as the Commission observed, "the complaint does not even seek to impose damages, let alone retrospective penalties." Comm'n Order Denying Resp't's Mot. to Dismiss at 17 (Jan. 16, 2014); *Riordan v. SEC*, 627 F.3d 1230, 1234-35 (D.C. Cir. 2010) (quoting *Drath v. FTC*, 239 F.2d 452, 454 (D.C. Cir. 1956)) (a cease-and-desist order preventing future misconduct is "purely remedial and preventative" and not a "penalty" or "forfeiture").

Respondent's claim that that the relief is not supported by the evidence, Resp't's Post-Trial Brief at 97, is equally without basis.[80] The Commission has wide latitude and considerable discretion in crafting its orders. CCCL ¶¶ 58-59. Injunctions issue based on the "'necessities of the public interest,'" balancing the interests of the parties who might be affected by the decision. *FTC v. Bronson Partners*, LLC, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (quoting *US v. Oakland Cannabis Buyers' Coop.*, 532 U.S. 483, 496 (2001)). Here, the interests to be balanced are the consumers' whose Personal Information LabMD holds, including consumers for whom LabMD performed no medical testing or other services, and LabMD's interests. As Complaint Counsel has demonstrated, LabMD's failure to maintain reasonable data security caused or is likely to cause substantial harm to consumers. CCFF ¶¶ 1472-1798.

---

[80] Respondent raises yet another fair notice claim. In addition to all the reasons previously stated, *supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-68; Argument, § II.C.1 (Section 5 Gives Fair Notice of Its Proscriptions), at 125-27, the cases on which Respondent relies do not support its claim. *See* CCRRCL ¶ 224.

The fact that LabMD has stopped accepting new specimens does not render the relief sought inappropriate. LabMD has no intention of dissolving as a Georgia corporation, retains the personal information of over 750,000 consumers, continues to operate a computer network, and intends to employ the same unreasonable policies and procedures to Personal Information in its possession as it employed in the past.[81] CCCL ¶¶ 60-64. These facts demonstrate that "'there exists some cognizable danger of recurrent violation,"[82] and entry of an order containing injunctive provisions is appropriate. *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (citing *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)); *see also FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1087-88 (C.D. Cal. 2012) (finding permanent injunction appropriate where defendant continued to work in same business field, even though no longer involved in the same type of conduct); *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1337 (M.D. Fla. 2010) (finding that defendant's new business venture in a similar industry "present significant opportunities for similar violations"); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393-94 (D. Conn. 2009) (imposing a permanent injunction where discontinued conduct was "obvious and widespread" rather than "a single instance" and "[f]uture violations of a similar nature would surely result in financial harm to consumers").

---

[81] Respondent claims that Dr. Hill evaluated LabMD's physical security and found it adequate. Resp't's Post-Trial Brief at 97. This is misleading at best. Dr. Hill's evaluation of LabMD's physical security was limited to LabMD's provision of locks to server rooms and physical access to LabMD computers. Hill, Tr. 293. Furthermore, the evidence shows that Personal Information is currently stored unsecured. (CX0713-A (Gardner, Dep. at 45-46) (paper records and patient specimens moved to Mr. Daugherty's residence; some items stored in a garage that was not always locked, and garage door was found up when Mr. Daugherty was not present)).

[82] This is the *only* standard Complaint Counsel must meet with regard to any future conduct by LabMD, Respondent's representation that Complaint Counsel must prove "that LabMD's past course of conduct is a basis for believing it will violate Section 5(n) in the future" notwithstanding. Resp't's Post-Trial Brief at 98.

The fact that Respondent issued a breach notice to consumers that were affected by the Sacramento breach does not render unnecessary the proposed Notice Order's requirement to notify individuals whose information was exposed. The proposed Notice Order would require LabMD to notify not only the health insurance companies of those who were affected by the Sacramento breach but also individuals whose information was exposed by LabMD's sharing of the 1718 File on the Gnutella network and their health insurance companies. *See* Proposed Notice Order, § III (requiring notification of Affected Individuals and their health insurance companies). LabMD has not notified individuals whose information was exposed in the 1718 File. *See* CCFF ¶ 1704.

The relief sought in the notice order, including establishment of a comprehensive information security program, the requirement to provide breach notices to consumers, document retention, and compliance reporting, is appropriate, as is the fencing-in relief of biennial assessments of Respondent's data security. CCCL ¶¶ 80-120. All of these provisions bear a reasonable relationship to the unlawful acts or practices alleged in the complaint and are sufficiently clear and precise for its requirements to be understood. *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965). The fencing-in provisions are necessary in this case because LabMD's data security failures were deliberate: it failed to heed warnings and demonstrated a pattern of carelessness and delay. CCCL ¶¶ 91-103. The violations were serious, as illustrated by the type of information collected by LabMD, the duration of its failures, and the security incidents involving the 1718 file and Day Sheets, CCCL ¶¶ 105-110. And the violations are transferrable, in that LabMD's practices continue to put the personal information of consumers – both the 750,000 consumers whose information it already has, and any future consumers whose information it collects – in jeopardy.

CCCL ¶¶ 112-114. Although there may be no evidence of prior violations of the FTC Act by LabMD, where failures are deliberate, serious, and transferrable, evidence of prior violations is not necessary to the appropriateness of fencing-in relief in an order. *Telebrands Corp. v. FTC*, 457 F.3d 354, 362 (4th Cir. 2006); *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012).

Finally, LabMD argues that the requirement to maintain a "comprehensive information security program" contained in the Notice Order is an impermissible "obey-the-law injunction," citing to *SEC v. Goble*, 682 F.3d 934, 949 (11th Cir. 2012). That case only stands for the proposition that an order cannot cross-reference provisions to statutes and rules that would require a defendant to have "compendious knowledge of the codes." *Id*. at 952. The Goble court vacated portions of an injunction only to remand the case so the district court could "specifically describe the proscribed conduct within the four corners of the injunction." *Id*. Here, the four corners of the comprehensive security program provision specifically describe the conduct required, and there is no basis to invalidate it. Indeed, the provision is consistent with the Commission's Safeguards Rule of the Gramm-Leach-Bliley Act, 16 C.F.R. § 314.1 *et seq*., with relief approved by the Commission in prior cases relating to unfair data security and other practices, with the Commission's guidance to businesses, CCCL ¶¶ 125-131, 146-155, and the Commission's prior issuance of consistent data security orders, CCCL ¶¶ 19-20.

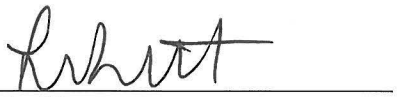
As to LabMD's restatement of its fair notice arguments, those are addressed elsewhere. *See supra* Argument, § I.C.1.a (Section 5 Provides Fair Notice of What Conduct is Unfair), at 62-68; Argument, § I.C.1.b (Mr. Kaufman's Testimony Did Not Violate the APA), at 68-68.

CONCLUSION

For the reasons stated in its post-trial brief, proposed findings of fact and conclusions of law, its post-trial reply brief, and its post-trial reply to Respondent's proposed findings of fact and conclusions of law, Complaint Counsel respectfully requests the Court to find that LabMD engaged in unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and to enter the notice order.

Dated: September 4, 2015

Respectfully submitted,



Alain Sheer
Laura Riposo VanDruff
Megan Cox
Ryan Mehm
Jarad Brown
Federal Trade Commission
600 Pennsylvania Ave., NW
Room CC-8232
Washington, DC 20580
Telephone: (202) 326-2999
Facsimile: (202) 326-3062
Electronic mail: lvandruff@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on September 4, 2015, I caused the foregoing document to be filed electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

I also certify that I caused a copy of the foregoing document to be served *via* secure file transfer to:

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

I further certify that I caused a copy of the foregoing document to be served *via* secure file transfer to:

Daniel Epstein
Patrick Massari
Erica Marshall
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
daniel.epstein@causeofaction.org
patrick.massari@causeofaction.org
erica.marshall@causeofaction.org

Reed Rubinstein
William A. Sherman, II
Sunni Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com
sunni.harris@dinsmore.com
Counsel for Respondent LabMD, Inc.

CERTIFICATE FOR ELECTRONIC FILING

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

September 4, 2015

By: _____

Jarad Brown
Federal Trade Commission
Bureau of Consumer Protection