ORIGINAL

PUBLIC

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

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

RESPONDENT LABMD, INC.'S
PRE-TRIAL BRIEF

William A. Sherman, II
Reed D. Rubinstein
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

Daniel Z. Epstein
Michael Pepson
Lorinda Harris
Hallee Morgan
Robyn Burrows
Kent Huntington
Patrick Massari
Cause of Action, Inc.
1919 Pennsylvania Avenue, NW
Suite 650
Washington, DC 20006
Counsel for Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Federal Statues

Federal Regulations

Federal Register

Administrative Materials

Other Authorities

INTRODUCTION

The Federal Trade Commission ("FTC") through its Bureau of Consumer Protection has brought this administrative action against LabMD, Inc. ("LabMD") claiming that it has violated the provisions of Section 5 of the FTC Act. The complaint focuses on the adequacy of LabMD's data security and its effectiveness in protecting the information which LabMD receives during the ordinary course of its business.

The FTC is aware that: LabMD is a medical laboratory; that medical laboratories are "covered entities" as that term is defined under the Health Insurance Portability and Accountability Act ("HIPAA"); LabMD receives only information related to health care and that such information is therefore "protected health information" ("PHI") as that term is defined under HIPAA; Congress gave specific authorization to Health and Human Services ("HHS") to enact legislation concerning the protection of health information; robust public notice and comment, including commentary from experts in the field of data security went into the enactment of the legislation; covered entities rely on the data security standards that have been established over the years through the enactment and enforcement of HIPAA; and the FTC has not published or otherwise made available to the public separate data security standards covering PHI.

Despite this knowledge the FTC takes the position that: HIPAA is not relevant to these proceedings; protected health information ("PHI") is not relevant to these proceedings; the data security standards that have developed within the medical industry under HIPAA are not relevant to these proceedings; and that the language of section 5 of the FTC Act is all that is required to put covered entities like LabMD on notice that data security measures for PHI over and above those required by HIPAA are necessary to comply with section 5 of the Act.

The FTC's position is untenable under the law.

In order to prove a violation of Section 5 of the FTC Act, the FTC must also prove that LabMD's actions have caused or 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. The FTC will not produce any evidence that any consumer has been harmed as a result of LabMD's data security practices. Despite the FTC's experts who conclude that as a result of LabMD's data security practices, a significant number of the individuals whose PHI appears on the documents that allegedly escaped LabMD's possession will experience financial or medical injury, there is no proof that any such injury has occurred or will occur.

STATEMENT OF FACTS

A. LabMD's Business

LabMD is a small, privately-owned medical services company providing cancer diagnoses through blood, urine, and tissue sample testing. Its customers are physicians. LabMD's business model consisted of the physicians sending samples to LabMD for testing and LabMD quickly returning the results and diagnosis to the physicians. Part of LabMD's competitive advantage was the process it designed to receive relevant patient identification and insurance information from its physician-clients electronically over a secure network. This process created quicker turnaround of results, less clerical errors in the medical records, less misdiagnosis, and saved hundreds of staff hours for doctor's offices involving patient information data entry. All information received, utilized, maintained and transmitted by LabMD is considered PHI as defined by HIPAA. *See* 45 C.F.R. § 160.103.

In fact, it is undisputed that LabMD is a HIPAA-covered entity. Opp'n to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Opp'n") (Nov. 22, 2013) at 22 fn 15; *see* 45 C.F.R. § 160.103. As such, it must comply with HHS' HIPAA and Health Information Technology for Economic and Clinical Health Act ("HITECH") regulations, including HHS' HIPAA Privacy Rule[1], HIPAA Security Rule,[2] and HHS' HITECH Breach Notification Rule.[3] HIPAA's Security Rule establishes substantive data security standards involving PHI with which HIPAA-covered entities, like LabMD, must comply. LabMD has never been accused of violating HIPAA or HITECH by the FTC, HHS, or anyone else. *See generally* Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, (Sept. 25, 2013)("Trans.").

B. Tiversa, Dartmouth, and The Insurance Aging File

The genesis of this action appears to have occurred in or about February 2008, when, without LabMD's knowledge or consent, Tiversa, Inc. ("Tiversa"), a government contractor that exploited data breaches to generate business, took possession of a single LabMD insurance aging file ("Insurance Aging file"). Compl., *Tiversa et al. v. LabMD et al.*, Dkt. 1, No. 2:13-cv-01296-NBF, at 4 ¶¶18-19 (W.D. Pa. Sept. 5, 2013)("Tiversa Compl."). After taking LabMD's property, Tiversa telephoned LabMD, "offered Tiversa's remediation services," and "provided[] a contract regarding the cost of remediation." *Id.* ¶¶19-21. That same day, Tiversa sent LabMD three emails following up on the phone call to sell its services. *See LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842, 843 (11th Cir. 2013).

[1] 65 Fed. Reg. 82,462 (Dec. 28, 2000).
[2] 68 Fed. Reg. 8,334 (Feb. 20, 2003).
[3] 78 Fed. Reg. 5,566 (Jan. 25, 2013).

Over the next two months, Tiversa sent six more emails soliciting business from LabMD. *See id.* Communications between LabMD and Tiversa stopped only when "LabMD did not retain Tiversa's services." Tiversa Compl. ¶22.

Tiversa has testified before Congress about its unique technology that monitors and interacts with peer to peer ("P2P") networks which enables Tiversa to search for sensitive information. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa, Inc.). Using this technology, Tiversa stated in a May 28, 2009, press release that in "a typical day" it might see sensitive information "of tens of thousands" being unknowingly "disclosed" by a hospital or medical billing company, a third-party payroll provider, or a Fortune 500 company. *See* RX485, Press Release, Tiversa, Tiversa Identifies Over 13 Million Breached Internet Files in the Past Twelve Months (May 28, 2009)("Tiversa Release").

In the Tiversa Release, Tiversa also stated that a Dartmouth College government-funded research project utilized its technology to search file-sharing networks for key terms associated with the top ten publicly traded healthcare firms in the country. According to Tiversa, they "discovered" what it called "a treasure trove of sensitive documents." *Id.* at 1. These included a spreadsheet from an AIDS clinic with 232 client names, including Social Security numbers, addresses and birth-dates, databases for a hospital system that contained detailed information on more than 20,000 patients, including Social Security numbers, contact details, insurance records, and diagnosis information. LabMD's Insurance Aging file was specifically mentioned and described as "a 1,718-page document from a medical testing laboratory containing patient social security numbers, insurance information, and treatment codes for thousands of patients." *Id.* at 1-2.

It could be that the LabMD file was the only file mentioned in the Tiversa Release that was given to the Commission. In the face of Tiversa's very public disclosures of supposedly massive patient-information data security breaches by large companies, it is not at all clear why the FTC singled out LabMD for an enforcement action, especially absent a complaining witness or evidence that the Insurance Aging file was in the possession of anyone other than Tiversa and the FTC.[4]

C. The Sacramento Incident

In October 2012, during a raid of a house of individuals suspected of stealing gas and electric utility services, the Sacramento Police Department ("SPD") found LabMD "day sheets" and copies of checks made payable to LabMD. Again, the day sheets and checks contained PHI from patients of LabMD's physician clients. CX0720, Jestes Dep. Tr. at 29-30, 33-36. In an

---

[4] LabMD believes that the 1718 file falls within the ambit of "improperly obtained evidence." As the Dissenting Statement of Commissioner J. Thomas Rosch to the Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 at 1-2 (June 21, 2012) states:

> Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing per se unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

LabMD believes the evidence at trial will show that Tiversa illegally obtained the 1718 file containing PHI and that the FTC was complicit in Tiversa's transfer of that file to a third party (the "Privacy Institute") run by a Tiversa board member whose studies were, in turn, funded by one of the FTC's testimonial experts in this case. The evidence will further show that the FTC then took possession of the 1718 file by sending legal process to the "Privacy Institute." The evidence will further show that this measure was taken to protect Tiversa's business reputation and economic interests. The evidence will further show that at all times relevant Tiversa, the Privacy Institute and the FTC knew or should have known that this scam "transfer" was improper or illegal because Tiversa did not own the PHI. The evidence will further show that Complaint Counsel concealed the true circumstances under which the FTC obtained the 1718 file from LabMD and from the Commission itself and that if the true circumstances been revealed, then Commissioner Rosch's concerns about the abuse of "prosecutorial discretion" would have been even more intense and compelling. If such is in fact the evidence, then the 1718 file and all of its fruits – that is, ***all* of the FTC's evidence of unfairness – should be excluded and this matter dismissed**. *Atlantic Richfield Co.*, 546 F.2d at 651 (stating rule).

attempt to notify LabMD of its find, the Sacramento police "googled" LabMD, and discovered that LabMD was under investigation by the FTC. *Id.* at 27-28, 56. The Sacramento police then notified the FTC of its find, but did not notify LabMD, despite Sacramento's awareness of LabMD's duty to notify under HIPAA. *Id.* at 28. Despite its duty to protect consumers, the FTC did not notify LabMD of the day sheets until approximately four months after it knew of their existence. RX15, Email from FTC to LabMD.

D. The Complaint

On August 28, 2013, the Commission voted unanimously to issue the Complaint, which alleges that LabMD violated Section 5's prohibition of "unfair" acts or practices by allegedly engaging in data security practices that, taken together, fail to meet the Commission's unspecified standards. *See Id.* ¶10. The Complaint does not allege that LabMD engaged in "deceptive" acts or practices. *See Id.* ¶¶22-23.

Instead, the Complaint alleges in vague, conclusory terms that LabMD engaged in unspecified "unfair acts or practices" and is replete with legal conclusions couched as factual statements. It does not cite any regulations, guidance, or other objective industry standards for what data security practices the Commission believes to be "adequate" or "readily available" or "reasonably foreseeable" or "commonly known" or "relatively low cost." *See id.* ¶¶10-11. It does not specify what regulations, guidance, or standards LabMD fell short of or what combination of LabMD's alleged failures to meet these unspecified requirements, "taken together," violate Section 5. *See id.* ¶¶10. It does not allege that LabMD's claimed "security failures" caused "consumers" to suffer any economic or other injury. *See id.* ¶¶10-11.

The Complaint cites two separate security incidents in an attempt to substantiate its claims. The first incident involves the Insurance Aging file. Specifically, the Complaint alleges

that "[i]n May 2008, a third party informed respondent that its June 2007 insurance aging report . . . was available on a P2P network through Limewire . . ." and that the "P2P insurance aging file contains personal information about approximately 9,200 consumers." Id. at ¶¶ 17-18. In any event, the FTC's Complaint does not allege that any "consumers" have suffered any harm due to the Tiversa taking.[5] *See* Compl. ¶¶17-19.

Secondly, the Complaint alleges that LabMD's "Day Sheets and a small number of copied checks" were found by the Sacramento Police "in the possession of individuals who pleaded no contest to state charges of identity theft." *Id.* ¶21. But it does not allege that those "individuals" in fact engaged in identity theft that caused any of LabMD's "consumers" to suffer any injury. *See id.* Instead, the Complaint alleges that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people with different names"—which, even if true, may be mere correlation (the Complaint does not allege any causation)—and speculates that this "**may indicate** that the SSNs have been used by identity thieves." *Id.* (emphasis added).

E. The FTC's Data Security "Standards"

When asked by the ALJ in this matter whether "the Commission issued guidelines for companies to utilize to protect...[sensitive] information or is there something out there for a company to look to," the FTC admitted that "[t]here is nothing out there for a company to look to." Trans. 9:13-18. The FTC has never promulgated patient-information data security regulations, guidance, or standards under Section 5 and, it has no Congressionally approved authority to do so: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act...for financial institutions." Trans. 10:11-15. LabMD is not a financial institution.

[5] As LabMD explained in its Answer, what the Complaint calls LabMD's "consumers" are in reality LabMD's referring physicians' patients. It is these physicians, and not their patients, who are LabMD's customers and the consumers of its diagnostic services.

Asked about other sources of data security standards, the FTC said the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC pointed to "public statements made by the Commission" and so-called "educational materials that have been provided" as standards. Trans. 9:23-25. In addition, the FTC argued that "the IT industry...has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7.

The FTC also referenced "guiding principles" and stated that "[t]here are lots of sources for the principles, such as materials published by the National Institute of Standards and Technology [NIST], continuing education for IT professionals, practical IT experience, and lessons learned from publicized breaches." Trans. 11:21-12:2. But critically, the FTC did not claim that any of the above has the force of law or creates any binding duties and obligations.

The FTC also accused LabMD of violating Section 5 "by failing to provide reasonable security for sensitive information," opining "that reasonableness is a common sense balancing of cost and benefit and that common sense is available from many, many sources, including organizations—government organizations, such as the National Institute of Standards, private entities, such as the SANS Institute, and many others as well." Trans. 21:20-22:2. But again, the FTC did not claim that LabMD violated any data security standards that have the force of law, such as the patient-information data security regulations implementing HIPAA.

In fact, the FTC has not accused LabMD of violating any data security statutes, rules, or regulations. At the hearing, the ALJ asked: "Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?" Trans. 22:10-12. The FTC responded "No." Trans. 22:13. The FTC also admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17.

After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data security "unfairness" offense are in this case. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data security standards—including "data security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present." RX518, Complaint Counsel's Resp. to LabMD's First Set Interrogatories, Int. 19.

Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions." *Id.* at Int. 21.

The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing discovery request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point

presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials.

Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are even dated after August 28, 2013, when the FTC issued this complaint. Yet Complaint Counsel's discovery responses, if taken at face value, suggest that there is really no standard, but instead a collection of thousands of pages of materials, statements and presentations related to data security, which must be gathered from a variety of sources, from which regulated entities such as LabMD are required to cobble together to divine the data security expectations of the FTC.

Complaint Counsel's pretrial brief and "Separate and Concise Statement of Material Facts as to Which There Exist Genuine Issues for Trial," read carefully, provide some clues as to what Complaint Counsel believes LabMD did wrong and confirms that Complaint Counsel is, in fact, holding out the paid expert reports of Dr. Raquel Hill as establishing the PHI data security standards LabMD, at all relevant times a HIPAA-covered cancer-detection medical healthcare provider, should have complied with.[6]

---

[6] LabMD will soon redepose the FTC Bureau of Consumer Protection Rule 3.33 witness on the issue of "what data security standards, if any, have been published by the FTC or the Bureau, upon which Complaint Counsel intends to rely at trial to demonstrate that Respondent's data security practices were not reasonable and appropriate." Order Granting Respondent's Motion to Compel Testimony (the "Rule 3.33 Order"), *In the Matter of*

F. LabMD's Data Security

The FTC has been unable to show which security standards or regulations LabMD failed to adhere, because LabMD's network "adhered to best practices" for security during the relevant time period. CX0950, Fisk Rep. at 33. From 2005-2010, LabMD had numerous features in place in order to protect the PHI which it received during the ordinary course of its business. Like most small businesses at the time, LabMD's infrastructure contained typical components: routers, switches, firewalls, servers, antivirus software, and employee computers. *Id.* at 16.

The most important security measures that LabMD had in place during the relevant time period were the "ZyWall" firewalls installed by Automated PC Technologies ("APT"). RX501, Hyer Dep. Tr. at 31, 58. All of LabMD's servers and equipment used firewalls to ensure security. *Id.* at 91. The ZyWall firewalls block incoming network requests while allowing outgoing requests, like almost any other firewall. CX0950, Fisk Rep. at 18. The ZyWall firewall was a commercial grade firewall which was recommended by APT because it met "fairly high industry standards with fairly good cost points." CX0731, Truett Dep. Tr. at 54. In fact, the ZyWall firewall was "more than adequate" to serve the security needs of a small business like LabMD. CX0950, Fisk Rep. at 20.

In addition to the firewalls installed, there was a Cisco router which had both sophisticated firewall and intrusion detection. CX0950, Fisk Rep. at 21. It was the routers which served as the gateways to LabMD's internal network, so their protective capabilities were important. The Cisco models used by LabMD were able to protect its internal network through an IOS firewall and IOS intrusion prevention system, "designed precisely for the type of small business network in place at LabMD." CX0950, Fisk Rep. at 21.

LabMD, Inc., FTC Dkt. No. 9357, at 6 (May 1, 2014). The FTC had previously refused to answer LabMD's questions about that issue. *See id.* at 3.

Within LabMD's internal network it supplied extensive precautions as well. LabMD employed a daily virus scanner whereby the TrendMicro antivirus would run a daily report and the IT employees at LabMD would work to resolve any issues it detected. RX486, Boyle Dep. Tr. at 126. The daily virus scans were routinely logged by APT so that the company could maintain the program properly. CX0731, Truett Dep. Tr. at 24. Moreover, LabMD's concern with patient safety led it to hire two companies, Providyn and Managed Data Solutions, to run penetration testing of its system to provide vulnerability analyses. RX486, Boyle Dep. Tr. at 34-35, 128. Whenever a critical vulnerability was detected through the testing, LabMD would work with the testing company to resolve the issues and ensure its clients' information was protected. *Id.*

As of 2001, LabMD had a policy giving employees computer accounts which restricted their ability to download files from the Internet and to install software on the computer. CX0950, Fisk Rep. at 22. The LabMD lockdown policy was described concisely in the Deposition of Robert Hyer:

> It's an access level or an authority level of what you can do on your PC to either add or change the use of applications. So a user could not install an application, could not install files without IT actually stepping in and doing it for them. So if they could justify a need for a new file, IT could install it but they couldn't.

RX501, Hyer Dep. Tr. at 148. Most departments had these internal firewalls which prohibited sites, but a few computers were able to avoid lockdown as a necessity for the job. RX508, Simmons Dep. Tr. at 54. However, even for the few computers which were not locked down, the affected employees were still expressly told they were not allowed to download anything without permission and LabMD had a stated policy against employees downloading things. *Id.* at 54, 94; RX74, Computer Hardware, Software, and Data Usage and Security Policy Manual, at 2. The

lockdown procedure prevented unwanted or unauthorized programs from coming on to the majority of LabMD employee computers because they were locked down.

The separate user accounts also increased security through passwords and limited the amount of internal information LabMD employees could see. The software employed by LabMD required each user to input a unique username and password in order to access the system. RX508, Simmons Dep. Tr. at 101. The credentials required to access the various software programs necessitated passwords of a certain length to be acceptable. RX486, Boyle Dep. Tr. at 149. Moreover, even a user's credentials would not give him or her access to the entirety of the database. *Id.* at 143. Instead users were restricted to information which was necessary for his or her job duties. RX506, Maire Dep. Tr. at 81.

While it is impossible to completely control the actions of the employees and clients, LabMD had policies in place to prevent the possibility a security breakdown. When LabMD's doctor's office clients submitted patient information, LabMD ensured that the transmission was done through a computer it provided via a secure FTP connection. RX508, Simmons Dep. Tr. at 127-128. LabMD worked to curtail any improper conduct by its employees as well having various security policies in place which were constantly updated and maintained. RX501, Hyer Dep. Tr. at 154. LabMD took the time to draft not only an employee handbook which it updated numerous times, but also a "Computer Hardware, Software, and Data Usage and Security Policy Manual" which prohibited employees from downloading files or using their employee computers for unauthorized purposes. RX508, Simmons Dep. Tr. at 94, 99.

On September 25, 2013, the FTC admitted at a pretrial conference that LabMD is not accused of violating applicable PHI data security regulations. Trans. at 22:10-13. Despite the FTC not

alleging HIPAA violations in the present suit, it is necessary to note that LabMD had a HIPAA compliance policy in place. RX508, Simmons Dep. Tr. at 97.

Overall LabMD's security practices were "reasonable and adequate to protect the PHI it possessed." CX0950, Fisk Rep. at 34. While there was not a foolproof way for a company to prevent an employee from installing an application without permission other than by putting such a policy into place, LabMD's security was reasonable and certainly not cause for concern. CX0731, Truett Dep. Tr. at 114; 126; 138. The FTC has admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward" which suggests that LabMD's policies are, in fact, reasonable and adequate. Trans. At 20:15-17.

ARGUMENT

A. Burden of Proof

"The parties' burdens of proof are governed by Federal Trade Commission Rule 3.43(a), Section 556(d) of the Administrative Procedure Act ("APA"), **and case law.**" *In re N.C. Bd. of Dental Examiners*, FTC Dkt. No. 9343, 2011 FTC LEXIS 137, *10-11 (F.T.C. July 14, 2011) (emphasis added). Under Rule 3.43(a), Complaint Counsel "shall have the burden of proof, but the proponent of any factual proposition shall be required to sustain the burden of proof with respect thereto." *Id.* at *11 (quoting 16 C.F.R. § 3.43(a)). Moreover, Complaint Counsel must prove its case by preponderant evidence. *In re Rambus Inc.*, 2006 FTC LEXIS 101, at *45 (Aug. 20, 2006) (citing *Steadman v. SEC*, 450 U.S. 91, 95-102, (1981)), rev'd on other grounds, 522 F.3d 456 (D.C. Cir. 2008), cert. denied, 129 S. Ct. 1318, (2009)). *See In re Automotive Breakthrough Sciences, Inc.*, No. 9275, 1998 FTC LEXIS 112, at *37 n.45 (Sept. 9, 1998) (holding that each finding must be supported by a preponderance of the evidence in the record);

In re Adventist Health System/West, No. 9234, 1994 FTC LEXIS 54, at *28 (Apr. 1, 1994) ("Each element of the case must be established by a preponderance of the evidence.").[7]

B. The FTC Cannot Prove by a Preponderance of the Evidence that LabMD's Data Security Practices were Unreasonable

1. Legal Standard

LabMD is solely accused of violating Section 5 of the FTC Act's prohibition against "unfair" trade practices. Compl.¶¶ 22-23; *see* 15 U.S.C. § 45(a). Thus, Complaint Counsel bears the burden of proving four elements. *See* 15 U.S.C. § 45(a), (n). As a threshold matter, Complaint Counsel must prove that the acts or practices alleged in the Complaint are "in or affecting commerce . . . ." 15 U.S.C. § 45(a). In addition, Complaint Counsel must prove each and every one of the three additional statutory elements set forth in Section 5(n) of the FTC Act:

> 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.

15 U.S.C. § 45(n); *see also* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("Policy Statement on Unfairness"), reprinted in *Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984). In applying Section 5 of the FTC Act to data security cases, the Commission has recently expressed that "the touchstone of the Commission's approach to data security is reasonableness." Comm'n Statement Marking 50th Data Sec. Settlement (Jan. 31, 2014), available at

---

[7] Ultimately, Complaint Counsel must prove its case by "substantial evidence." *Schering-Plough Corp. v. FTC*, 402 F.3d 1056, 1062-63 (11th Cir. 2005) (stating standard); *see id.* at 1170 (reversing Commission and noting that "the Commission relied on somewhat forced evidence," and, rather than accepting the ALJ's credibility determinations, relied "on information that was not even in the record"); *see also id.* at 1165 ("It would seem as though the Commission clearly made its decision before it considered any contrary conclusion."). They cannot do so.

http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf;[8] *see also* Complaint Counsel's Pretrial Brief, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 18 (May 2, 2014)("Complaint Counsel's Pretrial Brief"). Notably, Complaint Counsel asserts that "[a]s 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." Complaint Counsel's Pretrial Brief at 19. However, in this situation, due process requirements constrain how reasonableness is construed. *S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273 (5th Cir. 1981)("*S&H Riggers*") is directly on point.[9]

2. Reasonableness in Light of *S&H Riggers*

In *S&H Riggers*, the issue was whether a Commission can utilize a general and broadly worded regulation to impose standards more stringent than those customarily followed in an industry. *Id.* at 1283. This was a consolidated case where the petitioners were cited under 29 C.F.R. § 1926.28(a), the primary Occupational Safety and Health Act of 1970 ("OSHA")

[8] The Commission's January 16, 2014 Order also reads into Section 5(n) a "reasonableness" standard for determining whether LabMD's PHI data security practices constitute "unfair" trade practices prohibited by Section 5. *See* Order regarding LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 18-19 (Jan. 16, 2014)("MTD Order").

[9] Irrespective of whether the "reasonableness" standard passes constitutional muster in some cases, Complaint Counsel's application of the MTD Order's "reasonableness" analysis, as applied to LabMD in this case, violates LabMD's due process rights under controlling precedent. This issue was not addressed by the Commission's January 16, 2014 Order. Although the Commission's Order confirms the Commission's decision to evaluate LabMD's PHI data security practices using a "reasonableness" framework, see MTD Order at 18-19, it is silent as to what specific benchmarks LabMD's PHI data security practices must be measured against to determine whether they were "unreasonable," e.g., medical industry PHI data security practices health care providers of LabMD's nature and size used. Likewise, the Commission's Order is silent as to whether LabMD's PHI data security practices during a certain period in the "relevant time period," e.g., 2005, 2006, 2007, 2008, 2009, 2010, should be measured against medical industry PHI data security practices in May 2014, or should be measured against then-prevailing medical industry PHI data security practices. Because the Commission's Order is silent on these critical and practical questions, this Court may fill in the foregoing interstices of the Order. Courts are obligated to construe statutes to avoid constitutional problems if it is fairly possible to do so. *Boumediene v. Bush*, 553 U.S. 723, 787 (2008); *accord Nat'l Fed'n of Indep. Bus. v. Sebelius*, 132 S. Ct. 2566, 2600 (2012) (recognizing "duty to construe a statute to save it, if fairly possible"); *INS v. St. Cyr*, 533 U.S. 289, 300 (2001). This Court should apply these principles to the Commission's MTD Order.

regulation pertaining to personal protective equipment for employees in the construction industry, for failing to wear appropriate safety gear. *Id.* at 1275. 29 C.F.R. § 1926.28(a) states:

> The employer is responsible for requiring the wearing of **appropriate personal protective equipment** in all operations where there is an exposure to hazardous conditions or where this part indicates the need for using such equipment to reduce the hazards to the employees.

Id. (emphasis added). The petitioners contended that their employees were following common industry practices, while the OSHA Commission contended that employees failed to meet the standard set forth in 29 C.F.R. § 1926.28(a). *Id.* at 1276.

In deciding this case, the court reasoned that the generality § 1926.28(a) "mandates that it be applied only in such a manner than an employer may readily determine its requirements by some objective external referent." *Id.* at 1280. The court went on to say:

> In theory the standard formulated by the Commission might be adequate to meet requirements of due process. Although the reasonable person standard "is one of the most nebulously defined concepts in the law, it has been, and in all probability will remain, one of the rudimentary precepts of our law." Possibly a reasonable person standard that does not accept industry practice as controlling can give employers adequate notice of the requirements of § 1926.28(a). **The difficulty with the Commission's approach lies more in its application than its formulation. Without articulating in this or any other case the circumstances in which industry practice is not controlling or the reasons it is not controlling in any particular case, the Commission would decide ad hoc what would be reasonable conduct for persons of particular expertise and experience without reference to the actual conduct which that experience has engendered. In other words, the Commission would assert the authority to decide what a reasonable prudent employer would do under particular circumstances, even though in an industry of multiple employers, not one of them would have followed that course of action.**

Id. at 1280-1281 (internal cites omitted)(emphasis added).

Ultimately, the Court affirmed its previous holding in *B&B Insulation, Inc. v. OSHRC*, 583 F.2d 1364 (5th Cir. 1978), stating that "in the absence of a clear articulation by the OSHA commission of the circumstances in which industry standard is not controlling":

> [d]ue process requires that § 1926.28(a) be read to **incorporate an objective industry practice standard.** Accordingly, in order to sustain a citation under this regulation, the Secretary bears the burden of proving either that the employer failed to provide personal protective equipment to its employees under circumstances in which it is the general practice in the industry to do so or that the employer had clear actual knowledge that personal protective equipment was necessary under the circumstances.

Id. at 1275 and 1285 (emphasis added); *accord Fla. Mach. & Foundry, Inc. v. OSHRC*, 693 F.2d 119, 119-21 (11th Cir. 1982) (same; upholding ALJ's findings *because* those findings comported with the "petitioner's correct view of the law of this circuit" (emphasis added).

3. *S&H Riggers* as Applied to LabMD

This instant matter is directly analogous to *S&H Riggers.* Complaint Counsel predicates its ability to regulate the data security of **personal identifying information** on its broad powers enumerated in Section 5 of the FTC Act. However, Complaint Counsel has consistently ignored the fact that LabMD is a HIPAA-covered entity, and that the information at issue in this case is classified as **PHI – not personal identifying information**. Opp'n to Mot. to Dismiss, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, ("MTD Opp'n") (Nov. 22, 2013) at 22 fn 15; *see also* 45 C.F.R. § 160.103. Therefore, LabMD must comply with HHS' HIPAA Security Rule, 68 Fed. Reg. 8,334 (Feb. 20, 2003), which establishes comprehensive objective data security standards involving PHI.

Here, the FTC is attempting to enforce Section 5 of the FTC Act over and above the objective medical industry standards concerning PHI enumerated in HIPAA's Security Rule.

Section 5 of the FTC Act is similar to the OSHA regulation at issue in *S&H Riggers*, as it is "general and broadly worded" and incorporates a reasonable person standard. Likewise, HIPAA's Security Rule is similar to the objective construction industry practices identified in *S&H Riggers*. Thus, *S&H Riggers* stands for the proposition that the FTC "cannot impose standards more stringent than those customarily followed in an industry under as general and broadly worded [statute as Section 5 of the FTC Act]." *S&H Riggers,* 659 F.2d at 1283.

It cannot be disputed with any degree of credibility that, since its enactment, HIPAA has set forth the customs followed in the medical industry for securing PHI. Only after robust public notice and comment did HHS with the blessing of the United States Congress enact a comprehensive set of regulations setting clear and concise expectations for companies that receive and exchange PHI in the ordinary course of their business. Moreover, the instant matter presents a stronger set of facts than those the *S&H Riggers* Court relied on in reaching its conclusion that the objective industry standard controlled over the general and broadly worded regulation. In *S&H Riggers*, the petitioner's objective construction industry practice standards were not codified. Here, the objective medical industry practice standards concerning the security of PHI are codified under HIPAA, strengthening the application of the *S&H Riggers* holding to LabMD's facts.

Since, Complaint Counsel cannot establish that LabMD had "clear and actual knowledge" that additional PHI data security measures were "necessary under the circumstances" and then failed to act,[10] Complaint Counsel bears the burden of proving that LabMD failed to adopt data security practices that were customary in the medical industry during

[10] Furthermore, there is no evidence to support this theory.

the timeframe of the alleged violations. *S&H Riggers*, 659 F.2d at 1285; *see also B&B Insulation*, 583 F.2d at 1370.[11]

4. The FTC Cannot Prove by a Preponderance of the Evidence that LabMD Failed to adopt Data Security Practices that were Customary in the Medical Industry[12]

Complaint Counsel has unapologetically taken the position that it does not intend, nor is it required, to prove that LabMD's data security practices fell below the objective medical industry practice standard established by HIPAA and HITECH—and indeed affirmatively stated that it cannot and will not do so. For example, Complaint Counsel admits that LabMD is not accused of violating any of HIPAA's statutes or regulations. RX526, Complaint Counsel's Amended Response to LabMD, Inc.'s First Set of Requests for Admission, at 8-9 (Apr. 1, 2014); Trans. at 22:10-13; *see* Compl. ¶¶ 22-23. More recently, Complaint Counsel states in its Response in Opposition to Respondent's Motion for Summary Decision, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357 (May 2, 2014) that:

> [t]he fact that the Commission has not accused Respondent of violating the Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. 104-191, 110 Stat. 1936 (1996), or the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Pub. L. 111-5, 123 Stat. 115 (2009) has no bearing on this case.

Id. at 4-5, 9 n.4. In light of the decision in *S&H Riggers*, Complaint Counsel is incorrect.

Respondent asserts that Complaint Counsel cannot meet its burden as a matter of law. Complaint Counsel has offered no evidence as to what the medical industry data security standard practices are or were at any specific point during the relevant time frame for healthcare

[11] The *S&H Riggers* analysis is industry specific (*e.g.*, in that case, the roofing industry, or in our case, what is specific for the medical industry).

[12] To be sure, LabMD is not arguing that the FTC should seek, or is even able, to enforce HIPAA. Rather, LabMD contends that HIPAA's security rule sets forth objective medical industry standards.

providers of type and size of LabMD. Complaint Counsel has not accused LabMD of violating the medical industry data security statutes that apply to LabMD. MTD Order at 12 n.20 ("[T]he Complaint in the present proceeding alleges only statutory violations . . . ."); Trans. 22:10-13; RX526, Complaint Counsel's Amended Response to LabMD, Inc.'s First Set of Requests for Admission, at 8-9 (Apr. 1, 2014) (responses to RFAs 7-8). Moreover, Complaint Counsel has not identified any circumstances of which LabMD had actual knowledge that would require LabMD to implement data security measures beyond those normally used in the medical industry. Therefore, the FTC cannot prove by a preponderance of the evidence that LabMD's data security practices were unreasonable.

5. Even If This Court Fails to Adopt the Holding in *S&H* Riggers, LabMD's Data Security Policies were Reasonable

Black's law Dictionary defines the word "reasonable" as "fair, proper, or moderate under the circumstances." *Black's Law Dictionary* 1049 (8th ed. 2005). According to the FTC, a proper reasonableness analysis applied to the instant matter turns on whether LabMD's data security practices were fair, proper, or moderate in light of LabMD's compliance with "guidance available on how to identify the risks and vulnerabilities [it faces]." Complaint Counsel Pretrial Brief at 19.

Specifically the FTC states:

> A company can reference the recommendations of government agencies, such as the National Institute of Standards and Technology ("NIST"), well-known private sources, such as the SANS Institute and other information technology training institutes, and manufacturers of the software and hardware the company uses.

Id. at 20. Moreover, the FTC advises that:

> Companies may also review FTC complaints and consent decrees, *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *15 (D.N.J. Apr. 7, 2014) (noting that consent orders provide guidance to courts and litigants); see also Comm'n Order Denying Resp't's Mot. to Dismiss at 14 ("complex questions

> relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings"), which concern fundamental security elements, including: conducting risk assessments to identify reasonably foreseeable risks; assessing the effectiveness of existing security measures and adopting additional measures in light thereof; testing and monitoring security measures for effectiveness; and adjusting the measures appropriately.

Id.

Ironically, the FTC has yet to point to any specific public guidance issued by NIST, the Sans Institute, or the FTC (in the form of complaints or consent decrees) that would have placed LabMD on notice that their data security was unreasonable. In fact, when Daniel Kaufman was asked during Bureau of Consumer Protection's Rule 3.33 deposition about the data security standards the Bureau would use at the hearing to establish that LabMD's data security was inadequate, Mr. Kaufman was instructed not to answer. *See* Order Granting Motion to Compel Testimony, *In the Matter of LabMD, Inc.*, FTC Dkt. 9357 (May 1, 2014).[13] The fact remains that the FTC's conceptualization of LabMD's alleged data security failures is derived solely from the report and testimony of Dr. Raquel Hill, who relied on her "education and experience" in formulating her opinion. Complaint Counsel's Pretrial Brief at 20.[14] By the FTC's own admission, "unreasonableness" is not determined by the unpublished analysis of a single expert, but rather varies depending on the circumstances and should conform to practices set forth in public guidance. *Id.* at 19. As the FTC has failed to perform this inquiry, it cannot show by a preponderance of the evidence that LabMD's data security practices are inadequate.

In fact, during the relevant time period, LabMD had several data security measures in place, which when taken together can be construed as reasonable, including, but not limited to:

---

[13] Pursuant to this Court's Order dated May 1, 2014, Mr. Kaufman will be re-deposed on Monday, May 12, 2014 regarding the FTC's data security standards. As such, LabMD reserves the right to supplement its pretrial brief with future testimony provided by Mr. Kaufman.

[14] Admittedly, Appendix B of Dr. Hill's report generally identifies the NIST and Sans Institute websites, along with many others, as materials used in forming her opinion. CX0740, Hill Rep. at Appendix B; however, nowhere in her actual report does she identify any guidance from NIST or the Sans Institute that LabMD should have conformed to. Moreover, Dr. Hill did not consider any complaints or consent decrees in formulating her report. *Id.*

- a ZyWall Firewall which served to block incoming network requests while allowing outgoing requests, CX0950, Fisk Report at 18, and met fairly high industry standards. CX0731, Truett Dep. Tr. at 54.
- a Cisco router which also served as a firewall, coupled with intrusion detection capabilities. CX0950, Fisk Rep. at 21.
- TrendMicro Antivirus software which alerted IT staff to critical data security issues. RX486, Boyle Dep. Tr. at 34-35, 128.
- Software limiting which employees could download files and install software on their computer. CX719, Hyer Dep. Tr. at 148.
- Policies stating that employees could not use work computers for anything other than business related purposes, and could not download files or install software with the permission of IT. RX508, Simmons Dep. Tr. at 94, 99.

This is why LabMD's expert concluded that LabMD's data security practices were "reasonable and adequate" to protect the PHI it possessed. CX0950, Fisk Rep. at 16, 34.[15]

C. The FTC Cannot Prove by a Preponderance of the Evidence that LabMD's Data Security Practices were Unfair Pursuant to Section 5

1. Legal Standard

In order for the FTC to prevail on its allegation that LabMD violated Section 5 of the FTC Act, as previously explained, it must show that LabMD's data security practices "[1] cause[d] or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Notably, this test is conjunctive, and requires

[15] It is also worth noting here that the FTC's data security expert could not find that LabMD's data security was inadequate after July 2010. RX524, Hill Dep Tr. at 138-140.

the FTC to establish each prong by a preponderance of the evidence. *In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *133-35 (Aug. 5, 2009). Because, as explained below, the FTC cannot prove by a preponderance of the evidence that: (1) LabMD's data security practices caused or are likely to cause substantial injury to a consumer; and (2) a substantial injury to consumers would outweigh the countervailing benefits, prong 2 of the unfairness test also fails.

2. The FTC cannot prove by a preponderance of the evidence that LabMD's data security practices caused, or are likely to cause substantial injury to consumers.

The FTC alleges that LabMD's "failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information . . . caused, or is likely to cause substantial injury to Consumers." Compl. at ¶ 21. However, despite exhaustive discovery, the FTC is unable to substantiate its claim.

a. LabMD's Data Security Practices Have Note Caused Substaintial Injury to Consumers

As support for the fact that LabMD's data security practices have caused substantial injury to its consumers, the FTC cites to both the Insurance Aging file and the day sheets incidents. Compl. at ¶ 17-21. However, even after four years of investigation and an exhaustive discovery period, the FTC has yet to produce the name of a single consumer that alleges that it has been harmed by either the Insurance Aging file or day sheets incidents, or any other LabMD data security practice, despite having access to the resources of federal investigative agencies such as the FBI. It is also worth noting that the Insurance Aging file has allegedly been available on P2P networks for six years.

Most recently in the deposition of Daniel Kaufman, the Bureau of Consumer Protection's Commission Rule 3.33 witness, testified that he was unaware of any individual's names

appearing on the Insurance Aging file that have been the victims of identity theft. RX525, Kaufman Dep. Tr. at 89. Moreover, the FTC was forced to admit in its responses to LabMD's Requests for Admission "that the FTC has no complaining witness who says that his or her data was released or disclosed as the result of LabMD's allegedly unlawful data security practices." *See* RX520, FTC's Responses to LabMD's Requests for Admission, Admission 15. Because the FTC cannot show that LabMD's data security practice caused harm to any consumer, the FTC must attempt to substantiate the first prong of its Section 5 Unfairness test by proving that LabMD's data security practices are likely to cause substantial injury to consumers – which it cannot, as discussed *supra*.

b. LabMD's Data Security Practices Are Not Likely to Cause Substantial Injury to Consumers

i. The Insurance Aging File and Day Sheets Incidents

Essentially, the FTC asserts that because the Insurance Aging file and day sheets, which contain PHI, were exposed to the public, there is a potential that identified consumers are likely to be substantially injured in the future. *See generally* CX0741, Van Dyke Rep. and CX0742, Kam Rep. However, this conclusory assertion makes gargantuan leaps that defy the basic principles of logic, failing to account for how and when the public disclosure occurred.

For example, when asked if it mattered "how the insurance aging file was taken from LabMD," Van Dyke responded "[t]hat's something I haven't considered in my opinion." RX523, Van Dyke Dep. Tr. at 39. Van Dyke also admitted that while he was provided information that the Insurance Aging file was found on four specific IP addresses, he was unable to determine "who they belonged to, who owned them, and who had access to them." *Id.* at 43-46. Likewise, Kam testified that he had not relied on anything other than Robert Boback's testimony to bring

him to the conclusion that the IP addresses in question were being used for identity theft. RX522, Kam Dep. Tr. at 67-68.

Regarding "when" the Insurance Aging file and day sheets escaped the possession of LabMD, Van Dyke stated:

> Q So when the insurance aging file escaped the possession of LabMD did not figure into your considerations or analysis at all?
> A No, not when it escaped.
> Q Does your analysis have a temporal component as it relates to the insurance aging file?
> A No it does not.

RX523, Van Dyke Dep. Tr. at 41.

Perhaps neither Van Dyke nor Kam contemplated how or when the Insurance Aging file and day sheets escaped LabMD's possession because the FTC, itself, does not know. To be sure, no discovery taken to date explains this phenomenon. The only evidence the FTC has presented thus far is that Tiversa allegedly found and downloaded the Insurance Aging file via a P2P network from an IP address in San Diego, California, CX0703, Boback Dep. Tr., and that the day sheets were found in the possession of two individuals unrelated to LabMD's business who plead no contest to state charges of identity theft. CX0720, Jestes Dep Tr.; CX0085. It is worth noting that the FTC was made aware that there is no evidence that the two "identity thieves" involved in the day sheets incident had any direct connection with the receipt of the LabMD paperwork. RX472, Email: R. Yodaiken to K. Jestes, Subject: Update.

Thus, it is equally as likely that these files escaped LabMD's possession due to breaches of physical security as opposed to data security. There are numerous schemes in which a rogue employee could have devised to circumvent LabMD's physical data security in order to pilfer these files out of LabMD's possession. *See* CX0703, Boback Dep. Tr.; RX524, Hill Dep Tr. Numerous theoretical scenarios could involve breaches of physical security – not data security,

as contemplated by the FTC's Complaint. If the FTC cannot show how or when Insurance Aging file and day sheets escaped LabMD's possession, or more specifically that the Insurance Aging file and day sheets escaped LabMD's possession due to a data security failure, it cannot then make the gigantic leap to assert that LabMD's data security practices are likely to cause substantial injury to consumers, particularly in light of the fact that no consumers have been harmed.

ii. PHI Stored on LabMD's Network

More recently, the FTC also argues that LabMD's data security failures place all consumers whose PHI is on LabMD's Network at risk. Complaint Counsel's Pretrial Brief at 58. The FTC's experts conclude that "LabMD's failure to use reasonable and appropriate measures to prevent unauthorized access to [PHI] on its computer network creates and increased risk of disclosure of this information." *Id.* Essentially, the FTC argues that while this information has not yet been disclosed, there is a potential for disclosure because of LabMD's data security practices, and thus a likelihood that LabMD's data security practices will cause substantial injury to consumers.

However, this position fails to take into consideration that LabMD began winding down its operations in January 2014, and currently employs only two people – both who are authorized to access PHI, and one of whom is Mike Daugherty. *See* LabMD's Opp. to Complaint Counsel's Mot. for Sanctions, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at Exh. 1 Daugherty Affidavit (Feb. 20, 2014). Moreover, the FTC fails to consider that PHI is not stored on personal computers, databases, or applications. Rather PHI is only stored on the Lytec and LabNet servers, and that the Lytec server is the only server connected to the internet. CX0765, Respondent's Resp. to FTC's Second Set of Discovery, Int. 14-16. Thus, the likelihood of a

consumer being substantially harmed by LabMD's data security practices is greatly diminished. In fact, the FTC's own expert, Dr. Raquel Hill was unable to conclude that LabMD's data security practices were inadequate after 2010. RX524, Hill Dep. Tr., at 140.

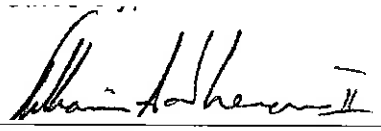
3. The FTC Cannot Prove by a Preponderance of the Evidence that a Substantial Injury to Consumers Would Outwieght the Countervailing Benefits

Any risk of storing patient information on LabMD's network has always been outweighed by countervailing benefits to consumers or to competition. LabMD's system of receiving and storing PHI provided a benefit to its customer physicians by creating quicker turnaround of results, less clerical errors in the medical records, less misdiagnosis, and saved hundreds of staff hours for doctor's offices involving patient information data entry.

CONCLUSION

The evidence at the evidentiary hearing will show that the FTC cannot prove by a preponderance of the evidence that LabMD violated Section 5 of FTC Act. Accordingly, Respondent respectfully requests that this Court enter an appropriate Order.

Respectfully submitted,



William A. Sherman, II
Reed D. Rubinstein
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004

CERTIFICATE OF SERVICE

I hereby certify that on May 9, 2014, I filed the foregoing document with the Office of the Secretary:

Donald S. Clark, Esq.
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 delivered via electronic mail and first-class mail 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 delivered via electronic mail and first-class mail to:

Alain Sheer, Esq.
Laura Riposo VanDruff, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq
John Krebs, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, NW
Mail Stop NJ-8122
Washington, DC 20580

May 9, 2014

By: _____
William A. Sherman, II
Dinsmore & Shohl, LLP