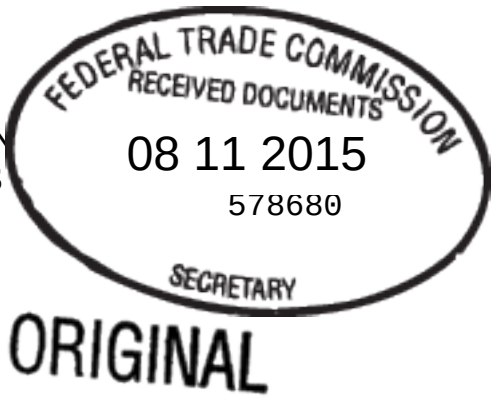
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES



ORIGINAL

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

RESPONDENT LABMD, INC.'S
CORRECTED[1] POST-TRIAL BRIEF

Daniel Z. Epstein
Prashant K. Khetan
Patrick Massari
Cause of Action, Inc.
1919 Pennsylvania Avenue, NW
Suite 650
Washington, DC 20006

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

Counsel for Respondent

Dated: August 11, 2015

[1] This document was timely filed on August 10, 2015. It is being re-filed solely to correct an error in the document due to the inadvertent inclusion of *in camera* information in yesterday's filing. Counsel for LabMD has been in constant discussion with Complaint Counsel as well as Crystal McCoy Hunter in the Office of the Secretary regarding these issues.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Statutes:

Other:

GLOSSARY OF TERMS

Administrative Law Judge	ALJ
Administrative Procedure Act	APA
Department of Health and Human Services	HHS
Federal Trade Commission	FTC or Commission
Federal Trade Commission Act	FTC Act
Health Insurance Portability and Accountability Act of 1996	HIPAA
Health Information Technology for Economic and Clinical Health Act	HITECH
LabMd, Inc.	LabMD
Peer to Peer	P2P
Section 5	15 U.S.C. §45
Sacramento Police Department	SPD
The Department of Health and Human Services	HHS
The Health Insurance Portability and Accountability Act	HIPAA
Tiversa, Inc.	Tiversa
United States House of Representatives Committee on Oversight and Government Reform	OGR

INTRODUCTION

The Federal Trade Commission ("FTC" or "Commission") has declared the Respondent, LabMD, Inc's ("LabMD") data security practices between January, 2005, and July, 2010, to have "caused" or be "likely to cause" substantial consumer injury and be "unfair" in violation of Section 5 of the Federal Trade Commission Act. *See* 15 U.S.C. §§ 45(a), (b) and (n). It has issued a Complaint and Notice Order to that effect.

Section 5(n) provides:

> 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. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

(Emphasis added.)

That LabMD has chosen to fight FTC, not to sign a consent order, sets this action apart at the threshold. "[I]n recent history Section 5 enforcement has resulted in no litigated cases and has instead focused upon administrative settlements chosen solely by the Commission."[2] Thus, this case raises multiple issues of first impression, including Complaint Counsel's burden of proof under Section 5(n). But it is the facts of the matter that make this case so truly remarkable.

This case has exposed FTC's reliance on a corrupt, crony "security" company called Tiversa, Inc. ("Tiversa"). Without a single real consumer victim, or one bare allegation of competitive impact, FTC has poured thousands of staff time hours and perhaps millions of

[2]Jan Rybnicek and Joshua Wright, *Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines*, 21 Geo. Mason L. Rev. 1287, 1305 (2014)(citations omitted).

taxpayer dollars into a snipe hunt for "unfair" and "unlawful" acts and practices that ceased between five and almost eight years ago and cannot reoccur. Without due consideration for the legal bases or unintended consequences of its actions, FTC has effectively declared that good faith compliance with the Department of Health and Human Services' ("HHS") Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulations for protected health information ("PHI") is no safe harbor and in this case would have such compliance declared unlawful.

This case has demonstrated that FTC will, in its zeal, ignore crimes (including at least one violation of Georgia's computer crimes law and multiple violations of 42 U.S.C. § 1320d-6(a), criminalizing unauthorized access to and distribution of PHI) and lies (by Tiversa and its CEO Robert Boback) to punish the victim. FTC's credulous collaboration with Tiversa demonstrates that it lacks both the technical expertise and the judgment needed to operate in the data security space. And, it raises the specter of government power being used to retaliate against a company for refusing to sign a consent decree and for criticizing the Commission and its staff, their motives, and their competence.

This case has produced a whistleblower's immunity grant. It has led to the recusal of one Commissioner and well-founded arguments for the disqualification of another. It has triggered an unprecedented Congressional investigation and hearing and highlighted the structural unfairness and constitutional infirmity of an enforcement system that has been described by a sitting FTC Commissioner as displaying "a strong sign of an unhealthy and biased institutional process" because "in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the

administrative law judge ruled found no liability, the Commission reversed…Even bank robbery prosecutions have less predictable outcomes than administrative adjudication at the FTC."[3]

And, in the end, this case has destroyed an innovative cancer detection firm, to the very real detriment of the doctors and patients who relied on it to provide a cancer diagnosis quickly and efficiently. The Commission's justification for all of this is, ostensibly, that LabMD's data security acts and practices between January, 2005, and July, 2010, viewed from the remove of years and disconnected from real-world medical industry practice, while turning a blind eye towards HIPAA, do not measure up.

That there was never a data breach in this case and LabMD met all of its obligations under applicable HIPAA regulations, apparently is of no moment.

As a matter of law, the Commission does not have the statutory authority to regulate PHI data security. This proceeding violates the Appointments Clause and Due Process provisions of the U.S. Constitution, is *ultra vires*, and arbitrary and capricious under the Administrative Procedure Act. Among other things, the Commission has ignored its obligations under 15 U.S.C. § 57(a).

Complaint Counsel has not proven causation or injury under Section 5, as cabined by Section 5(n) (including actual data breaches with statutorily-sufficient evidence of substantial consumer injury). It has not proven LabMD's data security is unreasonable and/or that the challenged pre-July, 2010, acts and practices are now causing or are likely to cause in the future substantial consumer injury that is not outweighed by countervailing benefits to consumers or to

[3] Joshua Wright, Commissioner, Fed. Trade Comm'n, Address at the Symposium on Section 5 of the Fed. Trade Comm'n Act: Time for the FTC to Define the Scope of its Unfair Methods of Competition Authority (Feb. 26, 2015) (Transcript *available at:* https://www.ftc.gov/system/files/documents/public_statements/626811/150226bh_section_5_symposium.pdf

competition, as the law requires it to do. It has not proven LabMD relied unreasonably on its data security experts. Finally, it has not proven the Notice Order is appropriate.

For these reasons, judgment for LabMD is proper.

FACTS

I. Background.

A. LabMD.

LabMD was a small, medical services company providing uropathology cancer detection services to physician customers. (Daugherty, Tr. 952). It was incorporated in 1996 by Michael J. Daugherty, its President and CEO and began primarily as a men's health clinic. (Daugherty, Tr. 939-40).

Prior to founding LabMD, Mr. Daugherty worked for 13 years in the hospital and healthcare field for Mentor Corporation as a Surgical Sales Representative for implantable devices used in Plastic Surgery including Urology. (Daugherty, Tr. 939-940). While working as a Surgical Sales Representative, Mr. Daugherty was "trained at US Surgical in Connecticut over a two–month period on aseptic technique, patient privacy, confidentiality, surgical technique" and "scrubbed in" with the surgeons. (Daugherty, Tr. 938).

In the 1990s LabMD changed its business model to meet a demand in the market for physicians who wanted their tissue samples analyzed by a pathologist who reads specific types of cells, which was made possible by mobile ultrasound machines. (Daugherty, Tr. 941–943). Managed care began requiring that physicians' offices direct tissue samples to a particular laboratory covered by the patients' health insurance. (Daugherty, Tr. 944–945).

LabMD's carved its niche by creating technology whereby physicians' patient databases were coded, so tissue sample requests could be sent to LabMD without physicians' staff needing

to spend time coding the samples by hand. (Daugherty, Tr. 959 - 960). LabMD created a process to streamline the interaction between physicians' offices requesting lab work and LabMD's delivery of the diagnosis of the lab work requested. (Daugherty, Tr. 955- 964). LabMD's process resulted in faster lab results turnaround time and fewer diagnostic code errors. (Daugherty, Tr. 961- 962).

The process was as follows:

- The tissue slides were received into the LabMD facility where a histologist put each sample into its proper cartridge. (Daugherty, Tr. 968; RXD 04). LabMD only analyzed one type of tissue, which allowed for 30-minute processing time as opposed to 12 hours. (Daugherty, Tr. 968–969).
- After the tissue is completely dehydrated, it was placed in an embedding center where hot wax wass poured over the sample to hold it firmly in place for cutting. (Daugherty, Tr. 969; RXD 06).
- The histotech then utilized the microtome "to cut the tissue one cell thick" for testing and analysis. (Daugherty, Tr. 969:21; RXD 07).
- The tissue was then placed "in a wax ribbon that is now one cell thick along the ribbon, and it's put in a water bath to rehydrate the tissue." (Daugherty, Tr. 970; RXD 08).
- A tissue slide was produced with identifying numbers showing case number and exact location within the gland. (". . . the last two digits are going to show the exact location within the gland. The top number in the center is the case number that is assigned electronically by the software back in the urologist's office when the nurse places the order. So at this point all these slides have had the proper, very legible information put on each one, so the correct tissue ribbon is put on each slide and they're ready to go to be

stained."). (Daugherty, Tr. 970– 971; RXD 10).

- The tissue sample wass then placed in the Sakura stainer which is part of the diagnosis protocol proper. (Daugherty, Tr. 971; RXD 11).
- The tissue slides were then taken out of the stainer "and will be started to be prepped for the physician's diagnosis to start." (Daugherty, Tr. 972; RXD 12).
- The tissue sample wass then placed into a final folder so the on-site physician at LabMD could begin "reading each slide location" and making a diagnosis. (Daugherty, Tr. 973; RXD 13).
- LabMD retained these samples and made them available for second opinions and or litigation purposes. (Daugherty, Tr. 972).

At all times during the relevant period LabMD's Employee Handbooks emphasized repeatedly that employees had a mandatory duty to protect PHI and that failure to do so would result in termination. (CX 0001 at 6). LabMD 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. (CX 0265; (CX 0704 (Boyle, Dep. at 92-109)). It sought and relied on expert advice and ran a compliant system. (CX 0704 (Boyle, Dep. at 12, 47-48,154-56)); (CX 0731 (Truett, Dep. at 32)).

B. LabMD Is Targeted By FTC/Tiversa.

In January, 2010, FTC attorney Alain Sheer called LabMD, informed it FTC was in possession of a computer file, and advised FTC would be initiating a non-public inquiry. Sheer promised a letter would arrive the next day. (Daugherty, Tr. 992-994).

This call, and many others like it, was the culmination of a purposeful, multi-year collaboration between FTC and Tiversa – the former to expand its regulatory authority and the later to further its shady and, at least with respect to PHI, criminal, business practices.

1. FTC and Tiversa

Tiversa was formed in 2004. (CX 0703 (Boback, Dep. at 10-12)). In July, 2007, Rick Wallace was hired by Tiversa as a forensic analyst. (Wallace, Tr. 1337- 1340).

In May, 2008, Tiversa contacted LabMD to sell it services by notifying it that the 1718 File had been "discovered" on P2P "networks." (RX 52; RX 53; RX 54; RX 55; RX 56; RX 57; RX 58; CX 21; (Daugherty, Tr. 985-987)). It wasn't until LabMD instructed Tiversa to direct any further communications to its lawyer that Tiversa ceased to press LabMD to purchase its services. (CX 59; (Daugherty, Tr. at 988-990)).

Wallace handled "special projects" for Boback. (CX0 872 (Gormely, Dep. at 83)). He scoured P2P networks and downloaded information from the Gnutella protocol networks. (Wallace, Tr. 1340). Wallace, while employed at Tiversa did confidential informant work for the FBI. (RX 0541 (Boback, Dep. at 63-64)). Wallace was highly skilled at retrieving data from P2P networks. (RX 0541 (Boback, Dep. at 100)).

Tiversa operated using a patented network platform and an array of servers. "Tiversa's platform was a series of algorithms that allowed the entire peer-to-peer network to be captured ***not going any deeper into any computer system*** but just has more breadth." emphasis added. (Wallace, Tr. 1340). Tiversa claimed that its technology enabled it view the entire P2P network "end to end" in real-time, viewing searches that others are making for data on the networks. (CX 0703 (Boback, Dep. at 99-101)). *Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the H. Comm. on Oversight Gov't Reform*, 110th Cong., at 20 (July 24, 2007)

(written statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last visited May 23, 2015).

Tiversa's "data store" was a depository of long servers containing data that is pulled in from different networks or peer-to-peer networks. Wallace explains that the data store is where Tiversa stored the information it pulled from the P2P networks. It contained the actual files and the IP addresses. (Wallace, Tr. 1371).

On February 25, 2008, Wallace, in the course of his employment, downloaded a LabMD insurance aging file that was 1,718 pages in length (the "1718 File") from a LabMD workstation located in Atlanta, Georgia at IP address 64.190.82.42. (Wallace, Tr. 1440-1441; CX 0307). Wallace would search and download files from the P2P networks, often without using Tiversa's search platform, and finding files that Tiversa's systems were not finding or catching. He describes how he found the 1718 file:

> "I was looking, using a stand-alone desktop computer, looking for a health insurance company who we were providing data service for. Again I was using that to supplement the—Tiversa's Eagle Vision, …so I was using that just to look and see if there's information that our systems were not downloading or catching.

(Wallace, Tr. 1372).

There were no written parameters used to decide what to download, because it was very difficult to know what was inside a file prior to downloading it. (Wallace, Tr. 1343). Wallace worked closely with Boback and would inform him when he made significant finds so he could decide how best to monetize it:

> Basically, I worked very closely at the time with Bob Boback. If it was something of -- significant in nature, then I would definitely go to Bob and say this is what we have, you know, and he would make the decision at that point how to best monetize that information, whether it be giving it to a salesperson or him calling the company directly.

(Wallace, Tr. 1344).

Tiversa began having difficulty selling its services and began contacting companies directly and charging them a lesser fee rather than a year long contract:

> early on, we were having problems at Tiversa, we were having problems selling a monitoring contract, so we started contacting individual companies when information came out, and you would be able to charge them a lesser amount than a yearlong contract, just basically a one-off to take care of that problem right then.

(Wallace, Tr. 1361).

Wallace prepared the materials used by Boback and Tiversa at a July 24, 2007 hearing before the United States House of Representatives Committee on Oversight and Government Reform ("OGR"), Chairman Henry Waxman presiding. (Wallace, Tr. at 1341- 1342); *see also Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. On Oversight and Gov't Reform,* 110th Cong. 1st Sess. 40-150 (written statement of Robert Boback, Chief Executive Officer, Tiversa, Inc.)(July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last visited Aug. 9, 2015).

Boback instructed Wallace to "use any and all means available to find information…[e]verything from health insurance information to PII, Social Security numbers, basically anything that should not be out on these networks." (Wallace, Tr. 1341 – 1342). Boback and Tiversa then lied to Congress when, on July 24, 2007, Boback stated to OGR that Tiversa's systems had obtained all files and information downloaded from P2P networks. Wallace testified:

> Q. [Mr. Sherman] And in the late 2007 when Mr. Boback was testifying before Congress at a hearing regarding peer-to-peer networks and identity theft, he asked you to help him prepare for that testimony; is that correct?
>
> A. [Mr. Wallace] Yes.

Q. And did you provide him with documents that you had found on the Internet long before ever joining Tiversa?

A. Yes.

Q. And at the time Mr. Boback testified at the congressional hearing, did he tell Congress who had found those documents?

A. Yes. He said that Tiversa's system had downloaded the documents.

Q. And that was not true, was it?

A. No.

Q. The documents, in fact, the majority of the documents that Mr. Boback referred to in his first congressional testimony in 2007 were documents that were identified by you rather than by Tiversa.

A. That's correct.

(Wallace, Tr. at 1432– 1433). (emphasis added); *see also Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform,* 110th Cong., 1st Sess. 88-106 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last visited May 20, 2015).

Mary Koelbel Engle, FTC's Associate Director for Advertising Practices in the Bureau of Consumer Protection, also testified. She affirmed FTC's long-standing position that P2P file sharing was like many other consumer technologies, a "neutral" technology. Ms. Engle continued, "[t]hat is, its risks result largely from how individuals use the technology rather than being inherent in the technology itself." In addition, Ms. Engle testified that:

> **Although [P2P filing sharing]** ***has required warnings with respect to inherently dangerous products, the Commission concluded that it was not aware of any basis under the FTC Act for requiring warnings for P2P file sharing and other neutral consumer technologies.***

Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1; 10; 40-84 (July 24, 2007) (written

statement of Mary Koelbel Engle on behalf of the FTC)(emphasis added); *see also* FTC Staff Report, *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues* at 20 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last visited Aug. 8, 2015).

FTC officials began contacting Boback and Tiversa approximately two months after this hearing. These contacts were frequent and would sometimes occur on a weekly basis. (Wallace, Tr. 1346 – 1347). FTC even personnel travelled to Pittsburgh for a demonstration of Tiversa's technology. (Wallace, Tr. 1351). Wallace's testimony that FTC's 2007 visit to Tiversa's facilities was infused with a "big wow factor":

> Q. What was the subject matter of those communications [beginning in 2007]? What did you talk about?
>
> A. We talked about information that was available on these networks. You know, ***there's always the big wow factor when people would visit our facility, like, you know, my gosh, I can't believe that this information is available for anyone to download.*** Then it – it went from there to providing information that only met a certain threshold that was relatively fluid at the beginning, but we were able to work through it.

(Wallace, Tr. 1349- 1350).

FTC then requested that Tiversa provide information that met a certain threshold which consisted of personally identifiable information exposed for greater than 100 people. (Wallace, Tr.1350 – 1351, 1562). Initially Tiversa refused to provide the requested information directly because of a pending acquisition. To create distance between Tiversa and the documents provided, (CX 0703 (Boback, Dep. at 142)); (RX 541 (Boback, Dep. at 37-38)), FTC and Tiversa agreed that the requested documentation would be provided to the FTC pursuant to a CID that would be served upon a then nonexistent third party, the Privacy Institute. (RX 525

(Kaufman, Dep. at 20)). Thus the Privacy Institute was created exclusively for the purpose of receiving FTC's CID and providing information. (Wallace, Tr. 1353); (RX 541 (Boback, Dep. at 38-41)).

Wallace prepared Tiversa/Privacy Institute's response to FTC in or about August, 2009. (Wallace, Tr. 1353- 1354). The list of approximately 90 companies (CX 0307) [4] was created by Wallace out of Tiversa's standard Incident Response Cases ("IRC"). Wallace explained that the IRC consisted of the names of companies whose information had been "found" by Tiversa on the P2P networks. The list was used by Tiversa salespersons and Boback himself to contact these companies to sell Tiversa's services. (Wallace, Tr. 1358- 1360).

The IRC "one-off" process at Tiversa was intended as a gateway to maximize Tiversa's profit by "monetizing" the PII and/or PHI in a way so as to create fear and intimidation for existing clients and intended target companies with whom Tiversa wanted to do business. (Wallace, Tr. 1360).

Boback decided upon and approved all of the companies on CX 0307 to maximize Tiversa's profits in acquiring new customers. He hoped that when these companies received letters from FTC they would call seeking Tiversa's services. (Wallace, Tr. 1362-1363). Although the threshold number for inclusion was 100 exposed consumers, Wallace testified that there were companies on the list with less than ten exposed consumers. (Wallace, Tr. 1362).

Wallace testified that many companies appeared on CX 0307, because they refused to do business with Tiversa:

> Q. When a company refused to do business with Tiversa, did Boback have a certain reaction to that?

[4]This document was identified as RX 0551 at trial because Wallace did not recognize the document in its redacted form.

A. Yes.

Q. What was that reaction.

A. Usually it would be something to the effect of they – you know, they – I've heard this said many, many times, that, you know, you think you have a problem now, you just wait.

(Wallace, Tr. 1364-1365).

Wallace was instructed by Boback to "use any means necessary to let [companies on the list] know that an [FTC] enforcement action is coming down the line and they need to hire us or face the music, so to speak." (Wallace, Tr. 1363). Boback further instructed Wallace to scrub the list of all past clients, "The list was scrubbed of all clients in the past and future clients that we felt that there might be, you know. The prospect of doing business with them. Their information was removed." (Wallace, Tr. 1362-1363). Boback and Tiversa retaliated against LabMD for refusing to engage Tiversa's services by placing LabMD near the top of the list of companies it turned over to FTC for enforcement proceedings and prosecution.

Q. [Mr. Sherman] ***Did Mr. Boback have a reaction to LabMD's decision not to do business with Tiversa?***

A. [Mr. Wallace] ***Yes.***

Q. And what was that reaction?

A. Do I say it?

MS. BUCHANAN: Answer the question.

A.***"He basically said [fuck] him, make sure he's at the top of the list.***"

Q. "What list?"

A. "This list in my hand (indicating CX 0307.)

(CX 0307; (Wallace, Tr. 1365-1366)) (emphasis supplied).

Wallace's list (exhibit CX 0307) contains LabMD's name and its IP address 64.190.82.42. It also contains a "date of disclosure" of February 25, 2008. (CX 0307).

FTC's revised *subpoena ad testificundum* to Tiversa was served via Federal Express on November 1, 2013. (CX 0029). Tiversa's production of documents pursuant to the subpoena included exhibit CX 0019. Exhibit CX 0019 contains the four IP addresses where the 1718 file was allegedly downloaded by Tiversa. (Boback, Dep. at 22-23)). Based on Complaint Counsel's document production, FTC supposedly first learned the 1718 File "spread" on the internet when CX 0019 was produced. *Compare* CX 0307.

CX 0019 was created by Wallace at Boback's specific command to make it appear as if LabMD's insurance aging file had spread or proliferated on the P2P network when in fact that was never the case. (Wallace, Tr. 1368-1370) (Q. "I submit to you that what's on your screen has been marked as CX 19 and has been admitted into evidence in this case." Q." What is that document?" A. "That is a list of IP addresses that was created in the November 2013 time frame of Bob came to me and basically said that him and LabMD are having it out, there's -- I didn't really follow the whole legal proceedings, but I knew that there was some bad water there. And Bob said that under no circumstances can the insurance aging file appear to have come from a 64 IP or in the Atlanta area. These IPs that are used here, these are all identity thieves that was provided from me to Bob. …" Q. "… So the purpose of creating the document in front of you was what?" A. "That was after Bob came to me and said that under no circumstances can the insurance aging file originate from a Georgia IP address or an Atlanta area IP address. And in addition to that, he told me to find an individual in San Diego to include with this list.") The false IP addresses, those of known criminals obtained by Wallace, as well as the date and time

the file was download, were "modified" and appended with LabMD's stolen insurance aging file, and injected into Tiversa's data store. (Wallace, Tr. 1374-1385).

Wallace also testified that he and Boback met with FTC officials, including attorney Alain Sheer. Wallace testified that after this meeting, Boback instructed him to make it appear that LabMD's insurance aging file had spread on P2P networks, when in fact that was never the case. (Wallace, Tr. 1386-1388) (Q. "Who traveled to D.C. [to meet with Alain Sheer and FTC] from Tiversa?" A. "Bob Boback was driving. I was in the car, Anju Chopra and Keith Tagliaferri." Q. "Following the meeting, did the people from Tiversa have discussions about the meeting?" A. "Yeah. I mean, we -- Bob spoke to me about next steps on the way home." Q. "And what were the next steps? …" A. "… Bob had indicated to me that the files needed to have spread on them, you know, basically look for them and see if they are available at other IP addresses, and if they're not, make them appear to have -- you know, be at different IP addresses.") (emphasis added); (A. "Yes. That was the purpose of the meeting, was to clarify the – how I put the data together, how it would correspond with the list and the actual file.") (emphasis added); (BY MR. SHERMAN: Q. "You testified that the purpose of the meeting was to discuss the information provided pursuant to the CID; is that correct?"
A. "Yes." Q. "And do you recall who was at the meeting?" A. "There were multiple people. I mean, I don't – I don't remember specific – I do remember Alain was there." Q. "Alain who?" A. "Alain Sheer.") (emphasis added).

At all times relevant, FTC knew, or should have known, the 1718 File was PHI. FTC also knew, or should have known, obtaining or disclosing same without the permission of the individuals listed thereon was a criminal violation of 42 U.S.C. § 1320d-6(a). FTC also knew, or

should have known, that FTC's "take" of the 1718 File from LabMD, as disclosed by CX 0307, was a facial violation of Georgia's criminal computer crimes law.

2. FTC Focuses on LabMD

Tiversa was Dartmouth's research partner. It aided Dartmouth by obtaining PHI (without authorization and in violation of 42 U.S.C. § 1320d-6) PHI and disclosing it (also without authorization and in violation of 42 U.S.C. § 1320d-6) to Dartmouth College so that Dartmouth College could conduct its federally-funded research (without authorization from the patients and so also in violation of 42 U.S.C. § 1320d-6). Tiversa was the source for Johnson's "Data Hemorrhages" article. (Johnson, Tr. 753-755); (CX 0872 (Gormley Dep. at 55-57)).

Tiversa, using its patented technology, began searching for PHI using Dartmouth's search terms in January, 2008, (CX 0382). It completed searching by January 28, 2008. (RX 371).

On February 25, 2008, Wallace, in normal the course of his employment, downloaded the 1718 File from a LabMD workstation located in Atlanta, Georgia at IP address 64.190.82.42. (CX 0307; Wallace, Tr. 1440-1441). In April, 2008, months after Tiversa stopped searching Dartmouth's search terms, Johnson requested that Gormley (a Tiversa employee) provide him with additional, perhaps new, information to help "spice up" and "boost the impact" of his work. (RX 371); (CX 0382); (CX 0872 (Gormley, Dep. at 69-71)). Neither Johnson nor Gormley would deny under oath that the 1718 File was the "spice" that "boosted the impact" of his article. (RX 483; Johnson, Tr. 772-774, 779-780); (CX 0872 (Gormley, Dep. at 103).

In May, 2008, Tiversa contacted LabMD to sell it services by claiming the 1718 File had been "discovered" on P2P "networks." (RX 052; RX 053; RX 054; RX 055; RX 056; RX 057; RX 058; CX 021; (Daugherty, Tr. 985-987)). When Tiversa refused to disclose the origin of the

1718 File, or how it came to be in possession of it, LabMD became suspicious and refused to buy. (CX 0059; (Daugherty, Tr. at 988-990)).

After the Tiversa sales call, LabMD immediately swept its system, discovered and removed the unauthorized LimeWire program, fired the individual (Rosalind Woodson) apparently responsible for the download as provided for by clear company policy, and searched (unsuccessfully) for the 1718 File on P2P networks to determine if it had spread. (CX 0704; Boyle, Dep. at 57-64); (CX 0730 (Simmons, Dep. at 10-11, 14-15, 99-100)).

On May 5, 2009, Boback once again appeared before Congress to testify regarding the dangers of P2P file sharing and data security. This time Boback displayed Respondent's 1718 file as part of his presentation. (CX 0703 (Boback, Dep. at 156)). *Hearing on H.R. 2221, the "Data Accountability and Trust Act," and H.R. 1319, the "Informed P2P User Act,"* Before the Subcommittee on Commerce, Trade and Consumer Protection, 111th Cong. (May 5, 2009)(statement of Robert Boback, Chief Executive Officer, Tiversa at 4, 10)(" most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not...On the FTC's website on the page "About Identity Theft," there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer's personal information…") *available at* http://democrats.energycommerce.house.gov/?q=hearing/hearing-on-hr-2221-the-data-accountability-and-trust-act-and-hr-1319-the-informed-p2p-user-a.

On July 29, 2009, Boback again testified to Congress. Wallace testified that part of Boback's testimony concerning highly sensitive information relating to Marine One being found at an IP address on the P2P networks, and was apparently downloaded by an unknown individual

in Iran was false. (Wallace, Tr. 1457-1458); *Inadvertent File Sharing Over Peer-to-Peer Networks: How It Endangers Citizens and Jeopardizes National Security*, Before the Committee on Oversight and Gov't Reform, 111th Cong. (July 29, 2009) (statement of Robert Boback, Chief Executive Officer, Tiversa, Inc. at 23) *available at* https://house.resource.org/111/gov.house.ogr.20090729.2.pdf.

FTC claimed it had "twenty-first Century law enforcement tools" to police P2P and the internet. *See* FTC, Mary Engle, *Prepared Statement of The Federal Trade Comm'n Before the Committee on Oversight and Government Reform United States House of Representatives* at 8 (July 24, 2007)("Combating twenty-first century consumer protection issues such as P2P file-sharing requires cutting-edge, twenty-first century law enforcement tools. For example, the FTC maintains Consumer Sentinel, a secure, online fraud and identity theft complaint database….[and] an Internet Lab, which provides FTC lawyers and investigators with high-tech tools to investigate high-tech consumer problems. It allows investigators to search for fraud and deception on the Internet in a secure environment. To capture web sites that come and go quickly, the lab also provides FTC staff with the necessary equipment to preserve evidence for presentation in court)" *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf . However, FTC did not verify Tiversa's claims or consider how Tiversa's obvious economic interest in aggressive FTC enforcement action might lead to abuse.

On February 22, 2010, FTC issued a press release titled "Widespread Data Breaches Uncovered by FTC Probe." *See* Press Release, FTC, *Widespread Data Breaches Uncovered by FTC Probe*, (Feb 22, 2010) *available at* https://www.ftc.gov/news-events/press-

releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last visited Aug. 9, 2015). In addition, the FTC published a guide for business warning about the dangers of P2P. The "FTC Probe" consisted entirely of taking information from Tiversa through the Privacy Institute and writing letters. And, even if the press release and business guide could be considered notice of the dangers of P2P in a business environment, it was published two years after the LabMD discovered and remove LimeWire incident.[5]

3. The LabMD Inquisition.

FTC began its inquisition of LabMD in January, 2010, based on Tiversa's theft of the 1718 File. By 2012, it had become clear to LabMD that FTC was more concerned about protecting Tiversa than about protecting its victims.

[5]In November, 2011, FTC put out a brochure containing what it then considered its five key data security principles. *See* FTC, "Protecting Personal Information: A Guide for Business," https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. The evidence is that during the January, 2005-July, 2010 time, LabMD complied with these principles, published years after the fact. For example, LabMD knew precisely what information it had received from its physician clients (Daugherty, Tr. 944–964); it kept only the patient information it received from the doctors, who determined the patients who needed to be prepopulated in the database to ensure accuracy and efficiency if that patient required testing in the future (Daugherty, Tr. 961- 962); LabMD had a secure network with firewalls, and antivirus software in place monitored and serviced by professionals (CX 0731 (Truett, Dep. at 31, 33, 41); (CX 0704 (Boyle, Dep. at 49-55)); and LabMD shredded all incomplete day sheets and aging reports (CX 0716 (LabMD Employee, Dep. at 62)); (CX 0714-A ([redacted] Dep. at 86, 54-55)); (CX 0706 (Brown, Dep. at 113-114)); (CX 0715-A (Gilbreth, Dep. at 63-68, 85-86); (CX 0006); (CX 0704); (CX 0730 (Simmons, Dep. at 16-17)). Of course, LabMD was fully aware of its regulatory obligations under HIPAA with respect to breach. Interestingly, these "principles" did not include Dr. Hill's "defense in depth," an approach that she claimed LabMD should have known about and employed in 2009. This allows only one of two conclusions: Either FTC's November, 2011, "five principles" were inadequate when issued and a data security system based on them would have been unreasonable; or Dr. Hill's "seven principles" were crafted in 2013 or 2014 specifically for the purpose of validating a predetermined outcome – that LabMD's data security between January, 2005, and July, 2010, was "unreasonable" and a violation of Section 5.

FTC sent LabMD a burdensome civil investigative demand. LabMD moved to quash arguing that the proceeding had been tainted by Tiversa's wrongful conduct. The Commission ruled against LabMD. However, Commissioner Rausch said:

> [The 1718 File] was originally discovered through the efforts of Dartmouth Professor M. Eric Johnson and Tiversa, Inc. In my view, however, as a matter of prosecutorial discretion under the unique circumstances posed by this investigation, the CIDs should be limited….**I am concerned that 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 [1718] File, and then repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD…the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

FTC's Statement Regarding Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands*:* Dissenting Statement of Commissioner J. Thomas Rosch at 2-3, FTC File No. 1023099 (June 21, 2012)(emphasis added).

FTC's lead witness was Robert Boback. Until CX 0019 and CX 0307 were produced, LabMD had never been told by FTC (or Tiversa) where the 1718 File had been "found." At all times relevant, however, FTC knew the truth. *See* CX 0307. Yet it never disclosed.

CX 0019 appeared shortly before Boback's deposition. (CX 0541 (Boback, Dep. at 22-23)). At Tiversa, "spread" or proliferation of P2P files on the Internet meant that the files were being reshared:

> Q. [Mr. Sherman] You mentioned the word 'spread.'
>
> A. [Mr. Wallace] Uh-huh.
>
> Q. What does that mean?
>
> A. That would be where a file is available and it appears to have been downloaded and being reshared to the network by multiple people.

Q. Isn't that a point of CX 19?

A. Yes.

(Wallace, Tr. 1385).

Tiversa's standard business model was to defraud existing clients and targeted future clients by fabricating spread:

Q. [Mr. Sherman] You testified earlier that when a company would refuse to do business with Tiversa, somehow their information would proliferate.

A. [Mr. Wallace] Yes.

Q. What do you mean by that?

A. Basically what happened would -- there needed to be a reason for Bob or somebody at Tiversa to contact that individual again or that company, so in order to use the -- you basically say that your file spread to a bad guy's IP address at, you know, Apache Junction, Arizona or wherever you could find a bad guy to put the file there as far as the system sees it, but it's really -- no data is transferring.

(Wallace, Tr. 1366- 1367). Wallace testified Tiversa created the illusion that companies' PII and/or PHI was widely available when it was not:

Q. [Mr. Sherman] Can you explain to us how you would make it appear as though the data had proliferated?

A. [Mr. Wallace] Sure. So as we talked about earlier, if you use a stand-alone client like a LimeWire or Kazaa or BearShare or whatever you have to supplement the data store with information, there is a folder that I would direct – or that I would put files in that would show up in the data store, you know, with Coveo or whatever application you're using to have a front end. It would show up just like it was downloaded from that IP. …

[JUDGE CHAPPELL]: Let me get this straight. … You actually did it. You actually made it available around the Internet in peer-to-peer —

A. No. No. We would only make it appear to have been downloaded from a known bad actor. So if you have an identity thief in Arizona, say, for example, we already know law enforcement has already dealt with that individual. We know that the IP is dead. We know that the computer is long

gone. Therefore, it's easy to burn that IP address because who's going to second-guess it.

[JUDGE CHAPPELL]: So to boil this down, you would make the data breach appear to be much worse than it actually had been.

A. That's correct.

(Wallace, Tr. 1367- 1368). Wallace testified Tiversa never "found" the 1718 File anywhere other than LabMD:

Q. [Mr. Sherman] In fact, the file was never – never spread anywhere on the Internet.

A. No. No. the originating source in Atlanta is the only source that it's ever been seen at.

(Wallace, Tr. 1443-1444)(CX 0370). Wallace inserted the IP addresses on CX 0019 into a folder designated "Input From Lab" and injected same into Tiversa's data store:

[JUDGE CHAPPELL]: … Could you tell by looking at your data store where the file actually had been seen or downloaded from as well as these IPs you had created to make it appear to be worse?

A. Yes. Because the folder where I would add that information to or the -- prepend the IP address to the file title, it would go into a separate folder that was called Input From Lab, so it wasn't stored in the normal directories that the rest of the files would be.

[JUDGE CHAPPELL]: "So you could -- you knew exactly where the file had been found, but how did you then show that to – let's say Company B didn't want to have a contract and you were told to make it look like the file was all over the Internet. How did you show that information to Company B? How did you demonstrate that?

A. Usually it would be after the fact, Bob would make contact with the company, without coming to me or coming to anyone else first, and say, you know, your file has spread to three additional IP addresses, it's in Europe and Nigeria and Poland and who knows. So then it would be up to me to make it appear 1 that way in the data store so, if there was ever an audit or, you know, somebody was catching on, the data would be there if you -- Coveo is basically a front end for the data store. It's like a Google site, so you could type in there 'insurance aging' and it's going to come up with a list of IP addresses along

> with the file, date and time. So in order to have that displayed, it needs to be inside the data store and indexed.
>
> [JUDGE CHAPPELL]: In the scenario you just gave me for fictitious Company B, when Mr. Boback told Company B that, that was untrue.

A. Yes.

(Wallace, Tr. 1373-1374) (emphasis added).

C. The Congressional Investigation.

The Chairman of the U.S. House Oversight and Government Reform Committee commenced a staff investigation of Tiversa over a period of months, also exploring FTC's relationship with that company, held a public hearing, and issued a report dated January 2, 2015 that was embargoed until after Wallace testified in open court. *See* RX 644 (not admitted for the truth of matters asserted therein). The staff investigation makes many notable claims, and purports to provide independent email and telephone record evidence to support same. (RX 644 at 16-18, 56-9, 62, 67). Certainly, FTC was aware Tiversa had a clear and direct economic interest in FTC action against the companies it turned over for enforcement action. *See* (CX 0679, Ex. 5 (Dissenting Statement of Comm'r J. Thomas Rosch, FTC File No. 1023099 (June 21, 2012), RX 644 at 56-9, 62, 67).

II. LabMD's Data Security Policies, Practices and Procedures.

A. Background.

During its investigation and throughout discovery FTC deposed many key LabMD employees and outside service providers in an attempt to gather sufficient proof that LabMD's data security practices, policies and procedures were unreasonable between 2005 and July, 2010. What FTC discovered was that during the Relevant Period each and every LabMD employee signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement indicating that they

had received the LabMD handbook and had an understanding of and compliance with LabMD's ethics policy and employment policy. (RX 336).

At all times during the Relevant Period LabMD's Employee Handbook contained "Privacy of Protected Information" language mandating compliance with HIPAA, with termination threatened for breach of PHI confidentiality. (CX 0001 at 6); (CX 0002 at 5-6). The Handbook contained the written policy that LabMD computers were to be used for company purposes only, including a prohibition against personal internet or email usage. (CX 0001 at 7); (CX 0002 at 7). Complaint Counsel's expert testified that these written statements within the LabMD handbook qualify as "policies of the company." (Hill, Tr. 289).

LabMD billing employees managers and non-managers alike testified consistently that LabMD had measures in place designed to protect PHI including written policies regarding HIPAA compliance, limited internet access, prohibitions against downloading from the internet, the shredding of aging reports, and limited ability to generate reports and print from the Lytec billing system. (CX 0716 (LabMD Employee, Dep. at 62)); (CX 0714-A ([redacted] Dep. at 86, 54-55)); (CX 0706 (Brown, Dep. at 113-114)); (CX 0715-A (Gilbreth, Dep. at 63-68, 85-86); (CX 0006); (CX 0704); (CX 0730 (Simmons, Dep. at 16-17)); (Boyle, Dep. at 39-48, 54-55, 68 - 71).

Billing employee Harris was employed by LabMD from October, 2006, through January, 2013, making her one of the longest tenured employees at LabMD. (CX 0716 (Billing Employee, Dep. 11)). Regarding LabMD's security policies and practices Billing Employee testified as follows:

- She describes her access to the internet as limited to insurance companies or otherwise being blocked. (CX 0716 (Harris, Dep. at 82-83)).

- She testified that on a yearly basis LabMD employees received training on LabMD compliance standards, HIPAA compliance, limited use of computer systems restricting use of internet and prohibition against playing CDs or downloading of information from the internet. (CX 0716 (Harris, Dep. at 62)).
- LabMD had in place user names and passwords for billing department employee computers with separate and different user names and passwords for the Lytec billing system. (CX 0716 (Harris, Dep. at 67-68)).
- Only billing personnel could access Lytec billing system. (CX 0716 (Billing Employee, Dep. 75)). It was necessary for billing personnel to have access to LabSoft in order to do their jobs. (CX 0716 (Harris, Dep. at 72-74)).
- The insurance aging reports were created and printed by the billing managers. The pages were divided amongst the billing department employees for the purpose of contacting insurance companies to collect unpaid balances. When they were finished using the portion of the report they had been given they would shred them. (CX 0716 (Harris, Dep. at 34-41)).
- She had no knowledge of a breach of the system during her tenure. (CX 0716 (Harris, Dep. at 130-131)).

Billing Employee[6] was employed by LabMD from 2007 through January, 2009. (CX 0714-A (Billing Employee, Dep. at 13)). Her testimony is consistent with that of Harris. Regarding LabMD's security policies and practices including the shredding of the insurance aging reports, Billing Employee testified as follows:

[6] Due to the confidential and sensitive nature of this witness' testimony the parties have agreed that her deposition is accorded in camera treatment and her name will not be used.

- Billing Employee received HIPAA training by watching a video on privacy concerns and HIPAA violations. (CX 0714-A ([redacted] Dep. at 86)).
- LabMD had in place user names and passwords for billing department employee computers and separate and different user names and passwords for the Lytec billing system as well as different user names and passwords for access to the LabSoft program. (CX 0714-A (Billing Employee, Dep. at 43, 45).
- It was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to bill denials of coverage for medically necessary tests. (CX 0714-A (Billing Employee, Dep. at 46-47)).
- The insurance aging reports were created and printed by the billing managers. They were used for the purpose of contacting insurance companies to collect unpaid balances. (CX 0714-A (Billing Employee, Dep. at 49-50)). When they were finished using the portion of the report they had been given they would shred them. (CX 0714-A (Billing Employee, Dep. at 54-55)).

LabMD billing employee Brown was the billing manager from May 2005 to May 2006. (CX 0706 (Brown, Dep. at 6-7)). From 2006 through 2013 she worked from home doing billing from insurance aging reports. Her testimony is consistent with that of Harris and Billing Employee regarding limited internet access and the necessity for billing employees to access Lytec and Labsoft in order to perform their jobs and the shredding of the insurance aging reports. Brown specifically testified as follows:

- Non-manager billing employees did not have the same access to Lytec as the managers had, because the non-manager employees could not print reports. (CX 0706 (Brown Dep. at 113-114)).

- Internet access was limited to the insurance company web sites and only managers had access to MicroSoft Outlook emails. (CX 0706 (Brown, Dep. at 115, 121).
- It was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to send information to insurance companies if they asked for medical records and for an appeals request (CX 0706 (Brown, Dep. at 117-118, 153).
- Insurance aging report pages were shredded. (CX 0706 (Brown, Dep. at 143-144)).

Another long tenured employee, Patricia Gilbreth, a billing manager, was employed from 2007 to 2013. (CX 0715-A (Gilbreth, Dep. at 6)). Her testimony is consistent with that of the other billing employees confirming that LabMD had measures in place to protect the information it possessed. Gilbreth testified as follows:

- There was annual training at LabMD about HIPAA and protecting information. (CX 0715-A (Gilbreth, Dep. at 77-78)).
- After becoming billing manager Gilbreth conducted training for new billing department employees which included the employee handbook and security handbook. (CX 0715-A (Gilbreth, Dep. at 82, 85)).
- The ability to create a print an insurance aging report was limited to a few people in the billing department. (CX 0715-A (Gilbreth, Dep. at 33-35).
- The aging reports were shredded. (CX 0715-A (Gilbreth, Dep. at 14-16))
- There were restrictions on access to the internet and there was a prohibition in the employee handbook against downloading from the internet. (CX 0715-A (Gilbreth, Dep. at 63-65))
- Gilbreth was familiar with portions of the LabMd policy manual and the “IT security

handbook" which was updated periodically. (CX 0715-A (Gilbreth, Dep. at 85-86); (CX 0006).

- There was a policy against personal email accounts. (CX 0715-A (Gilbreth, Dep. at 57)).
- Gilbreth considered the downloading of lime wire on Woodson's computer a security policy violation. (CX 0715-A (Gilbreth, Dep. at 67-68)).
- Gilbreth had no concerns and knew of no other employee who had concerns about LabMD's information security policies and procedures. (CX 0715-A (Gilbreth, Dep. at 67)).

LabMD IT employee Jeremy Dooley started with the company in 2004 and ended his employment in December 2006. He testified that during his tenure LabMD had firewalls installed to protect against intrusions and also installed antivirus software. (CX 0711 (Dooley, Dep. at 31, 71-72)). Both the lab software and the billing software had separate firewall routers. (CX 0711 (Dooley, Dep. at 24)). Security risks and vulnerabilities were assessed by an outside contractor. (CX 0711 (Dooley, Dep. at 38-39)).

John Boyle was employed as LabMD's Vice President of Operations and General Manager from November 2006 to August 2013. (CX 0704 (Boyle, Dep. at 7-8)). Boyle brought to LabMD an enormous amount of knowledge and experience in information technology and data security within the medical laboratory industry. Prior to joining LabMD Boyle worked for Cyto Diagnostics as a lab technician creating slides for urine samples, a DNA analysis lab technician creating computer generated reports and was promoted to team lead responsible for the entire process from receiving and processing the samples, staffing, writing and implementing policies and procedures and processes to qualify. (CX 0704 (Boyle, Dep. at 92-96)).

When Cyto Diagnostics changed its name to UroCor Boyle became the Accessioning Manager where he was responsible for receiving the samples either electronically or hard copy, applying the verification process ensuring patient data matches the sample and the appropriate testing is ordered before processing them through to the next department. As manager Boyle wrote the procedures for UroCor electronic accessioning process requiring interaction and coordination with operations, billing, finance, sales and pathology. (CX 0704 (Boyle, Dep. at 97-100)). Boyle was then promoted to the position of client relations interface manager where he interacted with the internal clients, the departments, and external clients, the physicians. (CX 0704 (Boyle, Dep. at 101-102)).

Later Boyle was promoted to the position of operations business analyst where he worked daily with the IT department on applications and structure to develop working product for segments of operations. (CX 0704 (Boyle, Dep. at 103-104)). Boyle was then moved into the IT department where he became the business analyst/information planning manager where part of his duties were to choose and implement a new billing and laboratory system giving consideration to that new system's ability to receive and process information electronically. (CX 0704 (Boyle, Dep. at 105-109)).

Boyle was then moved into the IT department where he became the business analyst/information planning manager where part of his duties were to choose and implement a new billing and laboratory system giving consideration to that new system's ability to receive and process information electronically. (CX 0704 (Boyle, Dep. at 105-109)). At that time Bob Hyer was director of IT at UroCor, and was a mentor to Boyle. Both worked together at UroCor in choosing the new billing and laboratory systems for UroCor. (RX 0501 (Hyer, Dep. at 17)); (CX 0704 (Boyle, Dep. at 110-111)).

When Uro Cor was purchased by DIANON and as a result Boyle became the Oklahoma City facility laboratory manager responsible for lab management over all departments in the facility while working with the IT departments for LabCorp and DIANON which involved planning, design review, coordination between IT departments and clients and interfaces. (CX 0704 (Boyle, Dep. at 112-113)). Later Boyle became the Director of operations for DIANON in 2003 through 2006 at which time external and internal transfers of protected health information were mostly conducted electronically and Boyle had the responsibility to ensure that those transfers were secure. (CX 0704 (Boyle, Dep. at 114-118)).

When Boyle joined LabMD in November of 2006 he described LabMD's system as being designed from the outside in making it efficient for the physicians to use. (CX 0704 (Boyle, Dep. at 123-125)). Boyle found the design of the transfer of information from clients to LabMD and the internal transfer of information within LabMD to be efficient and secure. (CX 0704 (Boyle Dep. at 125)). Information came to LabMD from physicians through a secure connection. (CX 0704 (Boyle, Dep. at 13)).

Boyle assumed oversight of compliance training for LabMD employees. LabMD's existing policies already prohibited employees, other than certain authorized IT personnel, from downloading programs or applications from the Internet. (CX 704 (Boyle, Dep. at 39-48, 54-55, 68 -71). When Boyle arrived Labmd's IT department was flat. There were no supervisors. (CX 0704 (Boyle, Dep. at 52-53)). IT personnel (including Curt Kaloustian, Alison Simmons and Chris Maire) reported directly to Boyle. (CX 0704 (Boyle, Dep. at 12); (CX 0685 (Boyle, Dep. at 154-56)).

Upon Boyle's arrival he found that LabMD had in place the Zywall firewall application installed by APT which was specific to APT's medical clients for Internet security; along with

security measures, including Internet access restrictions for non-managerial employees, TrendMicro anti-virus software and stratified profile setups, which limited the ability of employees to modify computer settings (there were three different levels: "Admin," "Local Admin," and "User level," for administrators, managers and line-level employee users). (CX 0731 (Truett, Dep. at 31, 33, 41); (CX 0704 (Boyle, Dep. at 49-55)).

Allen Truett's company APT would regularly be on site at LabMD managing networking, servers, hardware and applications. (CX 0704 (Boyle, Dep. at 47-48); (CX 0731 (Truett, Dep. at 32)). IT support services were provided by APT and internal staffing, and LabMD IT personnel implemented network upgrades and maintained the day-to-day monitoring and functioning of the network. (CX 0704 (Boyle, Dep. at 12, 39, 44-48).

Shortly after joining LabMD, Boyle reviewed LabMD's processes and procedures, including auditing the LabMD Administration department records and ensuring that all employees for whom there was not a signed acknowledgement document on file submitted a signed document acknowledging having read LabMD's Employee Handbook or Compliance policies. (CX 0704 (Boyle, Dep. at 71, 148).

Beginning in 2007, Boyle assumed oversight of compliance training. LabMD's existing policies already prohibited employees, other than certain authorized IT personnel, from downloading programs or applications from the Internet. (CX 0704 (Boyle, Dep. at 39-48, 54-55, 68 -71)).

In August 2007, LabMD implemented daily IT "walk arounds" to review the IT functions in all LabMD departments and, during the daily walk arounds, IT personnel visited each department daily and inquired if computers or computer accessories, such as printers, were showing any problems or errors. (CX 0704 (Boyle, Dep. at 73)). If a problem were reported or

observed, LabMD's IT personnel would attend to it immediately, on site. (CX 0704 (Boyle, Dep. at 39-48, 54-55, 68 -71)).

With all of these security measures in place on February 25, 2008, Rick Wallace downloaded the 1718 File from a LabMD workstation that was running a P2P file sharing program. (Wallace, Tr. 1441).

After being made aware that its file had been downloaded via a P2P file sharing program, and at Boyle's direction, LabMD IT employee Allison Simmons searched all computers at LabMD for file sharing software. She found no file sharing software on any other computer except for the billing manager Roz Woodson's computer. (CX 0730 (Simmons, Dep. at. 10-11)). Simmons removed the Lime Wire file sharing program from Woodson's computer. (CX 0730 (Simmons, Dep. at 14-15)). According to Simmons the billing department had a firewall and billing employees were prevented from going to non-specified web sites, except for those needed to perform their jobs. (CX 0730 (Simmons, Dep. at 16)).

Under Boyle's supervision and with his personal assistance, LabMD IT personnel (Simmons and Martin) immediately undertook a search of all other computers in the office and determined that *no other LabMD computers* contained either the LimeWire application or the 1718 File. (CX 0704 (Boyle, Dep. at 57-64)). To verify Tiversa's claims, Boyle instructed Simmons to search for the file on P2P networks from her home computer. Simmons searched for the file two hours on the day of the call from Tiversa and then once a week for a month or longer but was never able to find the 1718 file. (CX 0730 (Simmons, Dep. at 17-18)). Boyle assigned IT employee Simmons and later Martin to search P2P networks to find the 1718 file and they could not find the file on any P2P networks. (CX 0704 (Boyle, Dep. at 63-64))

As part of the investigation Simmons was asked to interview Woodson and determine her

knowledge of the program. Simmons concluded Woodson appeared to have no idea what the program was or whether she had shared files. (CX 0730 (Simmons, Dep. at 12, 93)). According to Simmons no one was supposed to download anything without going through IT. (CX 0730 (Simmons, Dep. at 17)). Woodson was terminated as a result of the P2P incident. (CX 0730 (Simmons, Dep. at 99- 100)).[7]

LabMD took additional and substantial measures to protect PHI. From August 2008 until June 2010, Boyle personally conducted walk arounds on a weekly basis, assisted by Robert Hyer or another IT employee, such as Matt Bureau. (CX 0704 (Boyle, Dep. at 39-40, 130-31).

From August, 2008, until June, 2010, Boyle and LabMD IT professionals physically reviewed each computer for the following: (1) the presence, function and updates of the TrendMicro security software; (2) MS Windows firewall security function and setup; (3) the profile set-up on each computer; (4) the installation and function of Windows security updates; (5) events recorded in the Event Viewer on the computer for errors in applications or function; (6) Internet Explorer history and use; (7) the deletion of temporary files in Internet Explorer, if applicable; (8) access to the correct network applications and servers; and, (9) Add/Remove programs to review the applications present on each computer. Through this process, LabMD checked the applications installed on each computer and verified that neither file-sharing applications, nor other unauthorized programs were on any LabMD employee's computer. (CX 0704 (Boyle, Dep. at 43-51, 70-71)).

LabMD hired Robert Hyer as the IT Manager in August 2009, at which time IT personnel began reporting to Hyer *and* Boyle, with Hyer reporting directly to Boyle as his immediate supervisor. (CX 0704 (Boyle, Dep. at 12; CX 0685 (Boyle, Dep. at 154-56)). Upon his arrival

[7]Oddly, FTC never deposed Woodson.

Hyer assessed that Curt Kaluostian was not qualified in any way to meet the demands of his position with LabMD. (RX 501 (Hyer, Dep. at 41 -42)).

LabMd was using TrendMicro or Symantec antivirus software. (CX 0704 (Boyle, Dep. at 43)). rendMicro is an overall security system with antivirus protection as one of its functions. LabMD had in place the current version of TrendMicro on its servers and desktops while it was in use during Hyer's tenure. (RX 501 (Hyer, Dep. at 164 -165)). The system was set up to limit access of physicians to their patients' information only. (RX 501 (Hyer, Dep. at 142)).

TrendMicro created reports and staff reviewed them. (RX 501 (Boyle, Dep. at 46)). Antivrus software was used on servers and workstations. (CX 0704 (Boyle, Dep. at 48)). LabMD had in place firewalls, routers, and Websense to protect its network. (CX 0704 (Boyle, Dep. at 49)). LabMD established policies regarding employees' passwords and access to information as there were controls by department, by function involving both lab and billing. (CX 0704 (Boyle, Dep. at 148-149)).

In May 2010, LabMD retained Providyn, Inc. to conduct quarterly scans of LabMD's servers and network. These scans were designed to search for and detect vulnerabilities in applications or in the network that could constitute a security threat. (CX 0704 Boyle, Dep. at 34-41)); (CX 0044-0084).

Under Hyer's direction LabMD addresses and resolves the critical risk items on the Providyn vulnerability scan assessments. (RX 501 (Hyer, Dep. at 108 -110)). Hyer concludes that a high priority item on the Providyn vulnerability scan assessment does not equate to a high probability of that risk actually occurring. (RX 501 (Hyer, Dep. at 110 -111)). During Hyer's tenure there were no security leaks or data breaches of point to point information being transferred between LabMD and its physician clients; scans of desktops were being run on a

daily basis; the security of the servers were tested on a weekly basis. (RX 501 (Hyer, Dep. at 156 -157)).

After June, 2010, and as defined in the desktop monitoring policy (CX 0006) all computers were monitored using a defined LabMD checklist**,** and were recorded upon a monthly basis by a Desktop Technician at LabMD. If the technician was providing support for any issue, including adding a printer or performing unscheduled maintenance on a computer, the technician reviewed the entire computer, including applications on the computer, to ensure that the computer's security was functioning in compliance with LabMD policies and procedures. (CX 0704 (Boyle, Dep. at 63-66, 68-70)).

In July, 2010, Boyle began conducting annual training on LabMD's Policy Manual, which memorialized policies previously in place at LabMD, including the prohibition on downloading files or software from the Internet. All LabMD employees are required to attend training on the Policy Manual. Each page of the manual was initialed by each person and each employee signed the signature page. Training records were maintained by the Administration department at LabMD. (CX 0704 (Boyle, Dep. at 68-70)).

LabMD IT employee Christopher Maire started with LabMD in mid 2007 and left in mid 2008 (CX 0724 (Maire, Dep. at 10)). Maire had a Bachelor's degree in Information Technology. (CX 0724 (Maire, Dep. at 106)).

Maire testified LabMD had written information security policies, employee handbook, HIPAA compliance and prohibition against personal use of company equipment during his tenure. (CX 0724 (Maire, Dep. at 18-19)). He routinely performed daily IT rounds to check on status of all computer systems. (CX 0074 – CX 0076); (CX 0724 (Maire, Dep. at 59)). During Maire's tenure LabMD also had written policies on, audit security operations, internet

connectivity policy, monitor security software settings and operating systems update policy. (CX 0006 at 8, 10, 13); (CX 0724 (Maire, Dep. at 21-23)). LabMD had a firewall intrusion-prevention system in place for the period 2007-2008. (CX 0724 (Maire, Dep. at 91)).

During the period 2007-2008, ClamWin was the antivirus software installed on LabMD's client's computers. (CX 0724 (Maire, Dep. at 95)).

During the period 2007-2008, LabMD had Windows antivirus software installed on its computer system. (CX 0024 (Maire, Dep. at 97)). Maire was not aware of any breach or occurrence of access to information by individuals not authorized to access such information. (CX 0724 (Maire, Dep. at 63-64)).

B. Fisk.

LabMD's data security expert Adam Fisk defines the Relevant Time Period for his expert report as January, 2005, through July, 2010. (RX 533 (Fisk, Dep. at 3)).

According to Fisk, LabMD's PHI data security was reasonable. (RX 533 (Fisk, Dep. at 32)). In fact, LabMD met a best practices standard. It had two layers of properly configured firewalls; there were proper user profiles on employee computers limiting the ability of non-managers to download files from the internet and to install applications. (RX 533 (Fisk, Dep. at 33)). The Cisco 1841 deployed at LabMD had both firewall and intrusion prevention capabilities and exceeded the FTC's best practices recommendation. (RX 533 (Fisk, Dep. at. 33)). The ZyWall5 IPSec firewall was a redundant layer of protection that shielded the LabMD network from unauthorized intrusion. (RX 533 (Fisk, Dep. at 33)).

LabMD did not deploy File Integrity Monitoring, however LabMD had a policy against employees installing applications not necessary for the performance of the job and performed regular checks on employee machines in an effort to ensure that employees adhered to that

policy. (RX 533 (Fisk, Dep. at 33)). According to Fisk, the best practices guidelines during the Relevant Period did not include File Integrity Monitoring in their recommendations. (RX 533 (Fisk, Dep. at 33)).

The 1718 File was not downloaded from LabMD through the firewall or due to any mis-configuration of LabMD's firewall. (RX 533 (Fisk, Dep.at 27)). LabMd's firewall was properly configured and performed just as it should have by blocking incoming connections. (RX 533 (Fisk, Dep. at 27)). Computers running LimeWire do not receive connection requests through the firewall because they are making outgoing connection requests to the Gnutella network. (RX 533 (Fisk, Dep. at 27)).

Fisk testified that due to Hill's limited understanding of how LimeWire works, Dr. Hill erroneously concluded that LimeWire was running as an application accepting incoming connection requests through the firewall. (RX 533 (Fisk, Dep. at 26-27));(CX 0740 at 43). Consequently, relying solely on the testimony of Mr. Kaloustian, she erroneously concluded that the 1718 File was taken because LabMD's firewall was either disabled or misconfigured. (CX 0740 at 36, 45).

III. The Day Sheets

On October 5, 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. The Day Sheets and checks contained PHI. (CX 0720 (Jestes, Dep. at 29-30, 33-36)). SPD attempted to notify LabMD of its find. However, Jestes searched "LabMD" and discovered that LabMD was under FTC investigation. (CX 0720 (Jestes, Dep. at 27-28, 56)). This was the investigation triggered by the 1718 File and Tiversa. Jestes informed FTC of the existence of the day sheets one week later. (CX 0720 (Jestes, Dep. at

61)). The Day Sheets were found in paper form, not electronic form. (CX 0720 (Jestes, Dep. at 58)).

LabMD was aware of its obligations under HIPAA to notify the patients listed on the Day Sheets and complied. (Daugherty, Tr. 1020-1021); (RX 348 (LabMD Patient Notification Letter [redacted])). LabMD's Day Sheets were not saved electronically. They were printed and made a part of batch reports. (CX 0714-A ([redacted] Dep. at. 65-66); (RX 497 (Gilbreth, Dep. at. 42-44)). They were found paper form, not electronic form. (CX 0720 (Jestes, Dep. at. 58)).

Complaint Counsel has not proven how the Day Sheets escaped LabMD's possession or how they ended up in California. (Hill, Tr. 220-221); (CX 0720 (Jestes, Dep. at 46)). Dr. Hill concluded that LabMD's physical security was adequate. (Hill, Tr. 293).

IV. Predicates To Relief.

Complaint Counsel has offered no evidence of any actual loss or harm (not fraud, identity theft, embarrassment or anything else) to any identifiable consumer or to competition due to the past "Security Incidents," LabMD's past data security acts or practices, or to LabMD's post-July, 2010, data security acts or practices. Compl. at 4-5.

Complaint Counsel has offered no evidence that the allegedly unfair acts or practices that occurred between January, 2005, and July, 2010, will, are likely to, or even can reoccur.

Complaint Counsel has offered no evidence of the medical industry data security acts and practices standards in effect during the time between January, 2005, and July, 2010,

Complaint Counsel has offered no evidence that LabMD unreasonably relied on its IT professionals and outside experts in developing and implementing its data security. This system was proven effective and useful over the years by LabMD's doctors, none of whom ever complained of a patient's identity theft, medical identity theft, or a HIPAA violation.

Complaint Counsel has offered no evidence that LabMD's allegedly unfair acts or practices were "serious" violations of the 15 U.S.C. § 45(a), *et seq*., or that there is the possibility the violations will "transfer," or any history of prior violations.

BURDEN OF PROOF/STANDARD OF REVIEW

Complaint Counsel bears the burden of proof. 16 C.F.R. § 3.43(a). The Commission does not sit as or with the authority of a court of equity. Instead it exercises only Congressionally-delegated administrative functions and not judicial powers. *FTC v. Eastman Kodak*, 274 U.S. 619, 623 (1927). The applicable burden of proof and standard for review therefore are dictated by statutory language.

Section 5 authorizes the Commission to prevent "unfair methods of competition." *See generally* 15 U.S.C. § 45. Section 5(b) authorizes the Commission to issue an order requiring the offender "to cease and desist from using such method of competition." 15 U.S.C. § 45(b). Section 5(n), which acts as a guard against FTC overreach, was enacted because FTC abused its power through "broad, unfocused, policy-based unfairness" claims. *See* J. Howard Beales, Former Comm'r, FTC, Address at The Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection." (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection. Section 5(n) provides:

> The Commission lacks 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 is not outweighed by countervailing benefits to consumers or to competition.

15 U.S.C. § 45(n).

Section 5's operative terms, including "unfairness," "causes," "likely" and "substantial injury," are undefined. Therefore, a common meaning construction is proper. *FDIC v. Meyer,* 510 U.S. 471, 477 (1994)(citing Black's Law Dictionary). Section 5 is titled "Unfair methods of competition unlawful; prevention by Commission." The construction of these terms will define the outer limits of the Commission's authority, and therefore must account for "the specific context in which that language is used, and the broader context of the statute as a whole." *Yates v. United States,* 135 S. Ct. 1074, 1081-83(2015)(Ginsburg, J.)(construing term "tangible object" in 18 U.S.C. § 1519 in the broader of the Sarbanes-Oxley Act and noting the section title and placement of the Act; Court read §1519 to cover only tangible objects, "one can use to record or preserve information" in opposition to the government's position that the term encompassed all evidence, including a fish); *see also Id.* at 91 (Alito, J., concurring)("my analysis is influenced by §1519's title… Titles can be useful devices to resolve 'doubt about the meaning of a statute'") (citations omitted).

Section 7 of the Clayton Act, 15 U.S.C. § 18, and Section 5 of the FTC Act "were enacted by the 63rd Congress, and both were designed to deal with closely related aspects of the same problem-the protection of free and fair competition in the Nation's marketplaces." *United States v. American Bldg. Maintenance Indus.*, 422 U.S. 271, 277 (1975). The lawful exercise of FTC's unfairness authority must connect to the "protection of free and fair competition in the Nation's markets." Beales, *supra* ("The Commission…is now giving unfairness a more prominent role as a powerful tool for the Commission to analyze and attack a wider range of practices that may not involve deception but nonetheless cause ***widespread and significant consumer harm***")(emphasis added). And at the threshold, the conduct must be "unfair." *See* S. Rep. No. 74-1705, at 2 (1936) ("[T]he Commission should have jurisdiction to restrain unfair or

deceptive acts and practices which deceive and defraud the public generally."); *id.* at 3 ("Under the proposed amendment, the Commission would have jurisdiction to stop the exploitation or deception of the public.")

Congress intended FTC's burden of proof to be very heavy and it designed Section 5(n) accordingly. *See*, S. Rep. No. 103-130, at 13 (1993) (stating that "[t]his section amends section 5 of the FTC Act to limit unlawful 'unfair acts or practices' to only those which cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition" and that "substantial injury" is "not intended to encompass merely trivial or speculative harm"); see also Statement of Rep. Moorehead, 140 Cong. Rec. 98 (Monday, July 25, 1994)("Taken as a whole, these new criteria defining the unfairness standard should provide a strong bulwark against potential abuses of the unfairness standard by an overzealous FTC--a phenomenon we last observed in the late 1970's."). As such, for FTC to lawfully exercise its Section 5 unfairness authority (as limited by Section 5(n)) against a given act or practice, it must prove that the targeted act or practice has a generalized, adverse impact on competition or consumers. *See Yates*, 135 S. Ct. at 1082-83, 85 ("we rely on the principle of *noscitur a sociis*—a word is known by the company it keeps—to 'avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress.'"); S. Rep. No. 75-22` at 2 ("where it is not a question of a purely private controversy, and where the acts and practices are unfair or deceptive to the public generally, they should be stopped regardless of their effect upon competitors. This is the sole purpose and effect of the chief amendment of section 5.").

I. **Causation**.

Section 5(n) does not authorize the Commission to declare unfair and order a respondent to cease and desist from an act or practice that "caused" past injury. 15 U.S.C. § 45(n). Instead, the Commission's unfairness authority is limited to an act or practice that "causes" substantial injury now or that "is likely to cause" substantial injury later. Consequently, where a case concerns past acts and practices (here, acts and practices that occurred between six and eleven years ago), Complaint Counsel must first prove a challenged act or practice is "likely" to reoccur – by definition, a past act or practice that is not "likely" to reoccur cannot be "likely to cause" future injury of any sort – and then that the act or practice in question is "likely" to cause substantial injury. *See United States v. W. T. Grant Co.*, 345 U.S. 629, 633 (1953)("[t]he necessary determination is that there exists some cognizable danger of recurrent violation, something more than the mere possibility which serves to keep the case alive")(citation omitted); *Borg-Warner Corp. v. FTC*, 746 F.2d 108, 110-11 (2d Cir. 1984)(holding FTC failed to bear its burden and justify relief because "conjectural speculation" was not sufficient to justify equitable relief against a terminated violation).

Congress did not define the term "likely," so the common meaning controls. Webster's primary definition of "likely" is "having a high probability of occurring or being true: very probable (rain is likely today)." *See* "Likely", Merriam-Webster's Dictionary, http://www.merriam-webster.com/dictionary/likely (last visited: Aug. 9, 2015). The Ninth Circuit has defined "likely" to mean "probable." *See Southwest Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1985)("likely" means FTC must show "probable, not possible" deception).

In turn, Webster's defines "probable" to mean "supported by evidence strong enough to establish presumption but not proof." *See* "Probable", Merriam-Webster's Dictionary,

http://www.merriam-webster.com/dictionary/probable (last visited: Aug. 9, 2015). Therefore, Complaint Counsel bears the burden of proving at the threshold (a) it is either probable or highly probable that LabMD's specific past acts and practices are not merely past, or (b) that there is a cognizable, not speculative or conjectural, danger that the past acts will reoccur, and then that those acts and practices will cause substantial injury.

Turning next to the issue of causation, in order to establish causation Complaint Counsel must prove three things by a preponderance of the evidence. First, Complaint Counsel must show that LabMD's PHI data security practices departed from the medical industry standards in effect during the relevant time. *S&H Riggers and Erectors Inc. v. OSHRC*, 659 F.2d 1273, 1283 (5th Cir. 1981).[8] Second, Complaint Counsel must show that 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. See MTD Order at 18-19. Finally, Complaint Counsel must show that LabMD's reliance on its IT professionals was unreasonable. *Fabi Construction Co. v. Secretary of Labor*, 508 F.3d 1077, 1083 (D.C. Cir. 2007)(citations omitted).

[8]The Order regarding LabMD's Motion to Dismiss, In the Matter of LabMD, Inc., FTC Dkt. No. 9357, at 18 (Jan. 16, 2014) (the "MTD Order"), does not preclude this Court from properly applying the *S&H Riggers* rule to test the evidence in this case because it was silent regarding the appropriate test and time-frame for "reasonableness" in this case. Thus, there is no law of the case barrier to a constitutionally proper burden of proof.

II. Injury.

Section 5(n) requires Complaint Counsel to prove that a challenged act or practice is "likely" (probable or highly probable) to cause "substantial injury" to consumers that is not reasonably avoidable by them or outweighed by countervailing benefits.

To begin with, Complaint Counsel must prove a substantial injury. In this case, that means Complaint Counsel must prove *both* actual data breaches *and* that LabMD's data security practices were "unreasonable" for medical companies during the relevant time frame. *See* MTD Order at 18; *S&H Riggers & Erectors, Inc*, 659 F.2d at 1283(mandating that reasonableness be tested according to prevailing industry standards). Proof of an actual data breach, due to an ongoing act or a past act or practice that is probable or highly probable to reoccur, is a necessary but not sufficient condition for "substantial injury" as a matter of law. [9]

[9]According to the Commission:

> Notably, the Complaint's allegations that LabMD's data security failures led to actual security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in 'unfair . . . acts or practices'….the mere fact that data breaches actually occurred is not sufficient to show a company failed to have reasonable "we will need to determine whether the 'substantial injury' element is satisfied by considering not only whether the facts [of actual data breaches] alleged in the Complaint actually occurred but also whether LabMD's data security procedures were 'reasonable' in light of the circumstances."

MTD Order at 18-19 (citations omitted).

The Commission's requirement of a data breach plus unreasonable practices is required by the *FTC Policy Statement on Fairness (1980),* as appended to *International Harvester Co.,* 104 F.T.C. 949, 1070 (1984)("FTC Unfairness Statement"). The FTC Unfairness Statement, as codified by Section 5(n), and is consistent with its practices in other cases. *See* FTC *v. Wyndham Worldwide Corporation*, 10 F. Supp. 3d 602, 609 (D. N.J. 2014). FTC's Unfairness Statement, to which Complaint Counsel is bound in this case, provides that "In most cases a substantial

Complaint Counsel must also prove that consumers could not avoid the injury and that the injury is not outweighed by any offsetting consumer or competitive benefits. FTC's Unfairness Statement provides the Commission exercises its unfairness authority "to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking" and analyzes the "net effects" of a challenged act or practice. Therefore, the Commission has bound Complaint Counsel to prove that LabMD, between 2005 and 2010, somehow unreasonably created or took advantage of an obstacle to the free exercise of consumer decisionmaking and that each challenged act or practice determined to be likely to cause harm is injurious in its "net effects."

III. Burden of Proof.

Complaint Counsel's burden of proof is, at a minimum, a preponderance of the evidence. *See In re N.C. Bd. of Dental Examiners*, FTC Dkt. No. 9343, 2011 FTC LEXIS 137 at *11-12 (F.T.C. July 14, 2011); *In the Matter of 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). However, the preponderance standard is inconsistent with a common-meaning construction of Section 5(n). If the term "likely" is given its ordinary dictionary meaning of "probable" or "highly probable," then Complaint Counsel

injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction." FTC Unfairness Statement. Unwarranted health and safety risks may also support a finding of unfairness. However, these "risks" must be proven "likely" to cause monetary harm in each case. *See* 15 U.S.C. § 45(n)(requiring current or "likely" future consumer injury). Only an actual data breach meets FTC's own criteria for substantial harm.

must prove its case by clear and convincing evidence. *Colorado v. New Mexico*, 467 U.S. 310, 316 (1984)(holding that a "highly probable" burden requires "clear and convincing" evidence).[10]

Complaint Counsel may not carry its burden using evidence obtained illegally or wrongfully or any of the fruits thereof. *Atlantic Richfield Co. v. Fed. Trade Comm'n*, 546 F.2d 646, 651 (5th Cir. 1977); *Knoll Associates v. FTC*, 397 F.2d 530, 537 (7th Cir. 1968) (remanding case to FTC with instructions to reconsider without documents and testimony given or produced by or through witness who stole materials from respondent). This is particularly true where the government abdicates its duty to investigate or corroborate evidence received from a third party. *United States v. Brown*, 500 F.3d 48, 56 (1st Cir. 2007)(authorities must at least "act with due diligence to reduce the risk of a mendacious or misguided informant"); *In re Big Ridge, Inc*., 36 FMSHRC 1677, 1738-39, 2014 FMSHRC LEXIS 465 (FMSHRC June 19, 2014)(Mine Safety and Health Review Commission excluded tainted evidence and found otherwise insufficient evidence to show violation of law); *Federal Trade Com. v. Page*, 378 F. Supp. 1052, 1056 (N.D. Ga. 1974) (recognizing deterrence of governmental lawlessness would be served by application of the exclusionary rule regardless of the criminal or administrative nature of the proceedings involved, and regardless of the personal or corporate nature of the party aggrieved by the unlawful seizure).

[10]Construing Section 5(n) by ordinary meaning, and requiring Complaint Counsel to prove causation and injury by clear and convincing evidence, is the only approach consistent with Congressional intent. *See* S. Com. Rep. 103-130 at 13 ("The Committee believes [Section 5(n)] is necessary in order to provide the FTC, its staff, regulated business, and reviewing courts greater guidance on the meaning of unfairness and to prevent a future FTC from abandoning the principles of the December 17, 1980, and March 5, 1982, letters"); Ernest Gellhorn, *Trading Stamps, S&H, and the FTC's Unfairness Doctrine*, 1983 Duke L.J. 903, 906, 942 (1983) (noting FTC's abuse of its Section 5 unfairness jurisdiction).

ARGUMENT

I. Constitutional And Statutory Infirmities.

Complaint Counsel's case is constitutionally and legally infirm for the following reasons.[11]

A. Appointments Clause.

Administrative law judges are "inferior officers" under the U.S. Constitution. U.S. Const. Art. II., § 2, cl. 2; *Freytag v. Comm 'r of lnternal Revenue,* 501 U.S. 868, 881 (1991); *Buckley v. Valeo,* 424 U.S. 1, 132 (1976). Therefore, they should be appointed to their position by "the President alone, by the heads of departments, or by the Judiciary." *Buckley, 424 U.S. at* 132.

However, FTC administrative law judges are appointed by the Office of Personnel Management. 16 C.F.R. § 0.14; *see also* Federal Trade Commission Website, *Office of Administrative Law Judges,* https://www.ftc.gov/about-ftc/bureaus-offices/office-administrative-law-judges (last visited Aug. 9, 2015) (administrative law judges are "appointed under the authority of the Office of Personnel Management"). Because ALJs are "officers" under the Appointments Clause, the "dual for-cause" removal protection afforded to them by statute is an unconstitutional "multilevel protection." *Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 484, 502 (2010); *see* 5 U.S.C. § 7521(a) (removal action "may be taken" by FTC against an ALJ "for good cause established and determined by the Merit Systems Protection Board"; 5 U.S.C. § 1202(d); 15 U.S.C. § 41 (FTC commissioners removable for cause).

[11]These are in addition to the arguments raised and rejected by the Commission and that are binding on this Court in the MTD Order, and which LabMD hereby specifically reserves. Also, LabMD specifically reserves all of the arguments raised in its various motions, including motions to dismiss and to exclude that were denied by the Commission and/or this Court.

As a matter of law, the Appointments Clause has been violated in this case. *See Hill v. S.E.C.*, Case 1:15-cv-01801-LMM, ECF 28, at 41-42 (N.D. Ga. June 8, 2015)(Holding that ALJs hearing administrative proceedings for the SEC "are inferior officers" within the meaning of the Appointments Clause and ruled that because the ALJ there was "not appointed by the President, a department head, or the Judiciary," the ALJ's appointment violated the Appointments Clause). Therefore, this case should be dismissed.

B. Statutory Preemption.

An agency may not use a general grant of authority to declare unlawful conduct that is permitted under a later and more specific legislative enactment. *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-71 (2012)(Where general and specific statutory authority simultaneously exist on the same topic, the specific governs). Therefore, the Commission's Section 5 authority must be viewed in the light of other relevant statutes, "particularly where Congress has spoken subsequently and more specifically to the topic at hand." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000); *see also FTC v. Nat'l Cas. Co.*, 357 U.S. 560, 562-63 (1958), superseded by statute (examination of subsequent statute and its legislative history demonstrates that it limits the FTC's Section 5 regulatory authority).

The Department of Health and Human Services ("HHS") is authorized to regulate medical data security, and has been for twenty years. *See* 42 U.S.C. § 1320d2(d)(1)("Security standards for health information"). It has promulgated data security rules specifically detailing what LabMD and other medical companies must do to protect PHI. *See, e.g.*, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334, (Feb. 20, 2003) (HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566 (Jan. 25, 2013) (HHS's HITECH Breach

Notification Rule); *see* 42 U.S.C. § 1320d-2(d)(1) ("Security standards for health information" established and enforced by HHS).

The preambles to HHS's HIPAA rules refer to the single national standard it creates. *See* 65 Fed. Reg. at 82,464 (This rule establishes, for the first time, "a set of basic national privacy standards and fair information practices"); 68 Fed. Reg. at 8,334(creating "national standards" to protect the confidentiality, integrity, and availability of electronic PHI).

Historically, the Commission has respected HHS' medical data security authority. For example, HHS has stated "entities operating as HIPAA covered entities and business associates are subject to HHS' and not the FTC's, breach notification rule." 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013). The Commission agrees. 74 Fed. Reg. 42,962-63 (Aug. 25, 2009)(FTC "received many comments about the need to harmonize the HHS and FTC rules to simplify compliance burdens and create a level-playing field for HIPAA and non-HIPAA covered entities" and so "FTC adopts as final the provision that the rule 'does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity'"); 964-65 ("HIPAA-covered entities and entities that engage in activities as business associates of HIPAA-covered entities will be subject only to HHS' rule" and not FTC's rule).

Congress does not allow the FTC to establish unfairness authority except through the procedure specified at 15 U.S.C. § 57a. However, FTC's health care breach notification rule was the result of a data security rulemaking pursuant to a specific Congressional grant of authority in the American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009). By necessary implication then, data security cannot fall under FTC's general unfairness authority. 15 U.S.C. § 57a.

The evidence in this case, which was not before the Commission when it issued the MTD Order, demonstrates that LabMD's data security acts and practices, though permitted by HHS, could be declared unlawful by the Commission through ad hoc adjudication. This necessarily interferes with the implementation of national regulatory standards for *precisely the same thing* – PHI data security.[12] Consequently, there is a "clear repugnancy" between HHS' standards and the Commission's actions here.

C. Due Process.

1. Fair Notice.

Complaint Counsel's failure to prove LabMD had adequate *ex ante* notice of what FTC prohibited and permitted with respect to HIPAA-regulated entities means this case should be dismissed for violation of due process. *See FCC v. Fox Television Stations, Inc*., 132 S. Ct. 2307, 2317 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required."); *Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)("traditional concepts of due process incorporated into administrative law preclude agencies from penalizing a private party for violating a rule without first providing adequate notice of the substance of the rule").

[12] According to Commissioner Wright:

> Whereas the common law process customarily depends upon numerous legal disputes initiated by adversarial parties to generate a fulsome body of judicial decisions that discover the correct application of the law, in recent history, Section 5 enforcement has resulted in no litigated cases and has instead focused upon administrative settlements chosen solely by the Commission. These disputes do not provide a sufficient basis for ascertaining when the Commission is applying Section 5 correctly; *rather they serve as de facto regulations that assert, on an ad hoc basis, when a practice represents an unfair method of competition.*

Rybnicek and Wright, *supra* at 1305-06 (citations omitted) (emphasis added).

The testimony of Daniel Kaufman, taken after the MTD Order was issued, demonstrates FTC failed its fair notice duty. (RX 532 (Kaufman, Dep. at 163-220)).

Kaufman cited consent decrees. A consent decree is not an agency standard. *Altria Grp., Inc. v. Good*, 555 U.S. 70, 53, 89 n.13 (2008)("…a consent order is in any event only binding on the parties to the agreement"). Kaufman cited "public statements," "educational materials," "industry guidance pieces" and even Congressional testimony as due process standards. (RX 532 (Kaufman, Dep. at 163-220)). But these are not legally sufficient. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006).

Kaufman did not establish standards, but he did establish FTC violates the APA. Agencies may not enforce statements of general policy and interpretations of general applicability except to the extent that a person has actual and timely notice of the terms thereof. *See* 5 U.S.C. § 552(a). Internet postings of "Guides for Business," links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication. *See* 5 U.S.C. § 552(a)(1)(D)(mandating Federal Register publication); *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001).

Fair notice also requires an objective, medical industry-specific "reasonableness" standard of care and not Dr. Hill's general "IT industry" standard. *See S&H Riggers,* 659 F.2d at 1280-81, 85; *Fla. Mach. & Foundry Inc. v. OSHRC,* 693 F.2d 119, 120 (11th Cir. 1982).

2. Tiversa/FTC Collaboration.

FTC's collaboration with Tiversa creates serious due process problems for Complaint Counsel. *See Withrow v. Larkin,* 421 U.S. 35, 47 (1975); *Gibson v. Berryhill,* 411 U.S. 564, 579 (1973).

To begin with, Tiversa should be deemed an "agent" of FTC, and FTC should be accountable for Tiversa's wrongdoing under the framework laid out in *Blum v. Yaretsky*, 457 U.S. 991 (1982) Among other things, FTC wrongly encouraged and ratified Tiversa's PHI take and disclosure in violation of 42 U.S.C. § 1320d-6(a). Obtaining and disclosing PHI without permission from the individual patient is a power reserved, if at all, to the government and not to a private company seeking to manufacture business. FTC empowered Tiversa. It should have shut it down.

Where evidence is obtained as the result of an "egregious constitutional violation" the exclusionary rule is permitted in federal administrative proceedings. *Oliva-Ramos v. Att'y Gen. of the United States*, 694 F.3d 259, 272 (3rd Cir. 2012); *see generally* Richard M. Re, *The Due Process Exclusionary Rule*, 127 Harv. L. Rev. 1885 (2014) (exclusionary rule is truly a due process rule).

Evidence illegally obtained is properly excluded in administrative proceedings. *Donovan v. Sarasota Concrete Co.*, 693 F.2d 1061 (11th Cir. 1982)(OSHA citation hearing). Due process forbids Complaint Counsel from using evidence provided by Tiversa in this proceeding. The exclusionary rule also forbids Complaint Counsel and its experts from reliance on its "fruits." *Atlantic Richfield Co.*, 546 F.2d at 651; *Knoll Associates* 397 F.2d at 537; *see also Rochin v. California*, 342 U.S. 165, 172-74 (1952); *see also Communist Party of the United States v. Subversive Activities Control Bd.*, 351 U.S. 115, 125 (1956).

As the court held in *Knoll Associates*:

> We hold that we have not only the power but the duty to apply constitutional restraints when pertinent to any proceeding of which we have jurisdiction, such as a statutory review of a federal commission decision. At stake here is the ordered concept of liberty of which Mr. Justice Holmes spoke in his dissenting opinion in Olmstead v. United States, 'apart from the Constitution the Government ought not to use evidence obtained and only obtainable by a criminal act.' In the same case, Mr. Justice Brandeis, likewise

> dissenting, said at 479: 'Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent….The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.' And, at 485, Mr. Justice Brandeis added: 'Decency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy.' This principle, thus announced in dissenting opinions, has since been recognized by the Supreme Court as presently the law of the land.

Knoll Associates, 397 F.2d at 536-537 (citations omitted).

For its commercial benefit, and in violation of applicable laws, Tiversa stole the 1718 File. *See* Ga. Code Ann. §§ 16-9-90 et seq.; 18 U.S.C. § 1030; 42 USC § 1320d-6; (Wallace, Tr. 1367-1396, 1399-1403, 1409-11). It provided same to Johnson and Dartmouth, in violation of 42 U.S.C. § 1320d-6, each of whom also benefited commercially from access to PHI. Finally, knowing Tiversa benefited commercially from government action, and as part of a larger effort to work with and profit from Tiversa's violations of law, FTC facilitated or directed Tiversa to transfer the 1718 File in violation of 42 U.S.C. § 1320d-6 to the Privacy Institute. (CX 0703 (Boback, Dep. at 142-143)); (RX541 (Boback, Dep. at 36-42)).

FTC's inquisition of LabMD, and all of the evidence it has introduced in this case, is the fruit of Tiversa's illegally activity as evidenced by the following:

- As FTC knew or should have known, Tiversa illegally obtained, reviewed and disclosed the 1718 File in violation of Georgia and federal law, whether or not LimeWire was running (contrary to company policy) on a LabMD computer. *See* 42 U.S.C. § 1320d-6(a) (knowingly obtaining or disclosing individually identifiable health information maintained by a covered entity without authorization is a felony).

- According to Tiversa, FTC directly colluded in violating 42 U.S.C. § 1320d-6(a) by way its role in creating the Privacy Institute and its civil investigative demand thereto.
- The record shows that Tiversa used FTC for its own financial gain so that it could pressure prospective clients under the threat of enforcement proceedings. (Wallace, Tr. 1363) (stating that Tiversa turned over potential clients to the FTC "so that the FTC would contact them and notify them of a data breach and hopefully we would be able to sell our services to them"); (Wallace, Tr. 1363). Tiversa included prospective client names on the list to turn over to the FTC as they would "use any means necessary to let them know that an enforcement action is coming down the line and they need to hire us or face the music, so to speak"); (Wallace, Tr. 1452-1453) (after Tiversa began working with the FTC, it threatened prospective customers with FTC enforcement proceedings). FTC knew this from the start. (CX 0679, Ex. 5 (Dissenting Statement of Comm'r J. Thomas Rosch, FTC File No. 1023099 (June 21, 2012)).
- The record shows Complaint Counsel knew the true origin of the 1718 File at the time it was produced by the Privacy Institute, and so it knew or should have known that CX 0019 and Boback's testimony in support thereof, were false and perjured. (CX 0307). Nevertheless, Complaint Counsel solicited and obtained expert testimony in this case using such false evidence and perjured testimony. Incredibly, Complaint Counsel has admitted never taking any steps to corroborate Tiversa's claims or using its "21st Century" law enforcement tools to verify whether the 1718 File had spread as Boback testified in his deposition.

Given FTC's past reliance on Boback in this case, its continued enforcement proceedings violate due process. *See Giglio v. United States,*, 405 U.S. 150, 153 (1972); *Morris v. Ylst*, 447

F.3d 735, 744 (9th Cir. 2006). FTC knew Boback lied no later than May 30, 2014, and disclosed that there was a "discrepancy" in Boback's testimony on that date. (Van Druff, Tr. 1227). However, the evidence suggests that Complaint Counsel knew or should have known that the long-held information contained in exhibit CX 0307 was diametrically opposed to the information contained in CX 0019 - which was produced on or about November 2013 in advance of Boback's deposition. In failing to investigate the accuracy of Boback's November deposition testimony concerning exhibit CX 0019, the FTC allowed this administrative action to continue in violation of LabMD's due process rights when its investigation had persisted since the production of CX 0307 in the absence of any documentation associating the 1718 file with any IP address other than that belonging to LabMD (64.190.82.42).

FTC was obligated to take appropriate steps to protect the integrity of this proceeding (and LabMD's rights). *See United States v. Basurto*, 497 F.2d 781, 785 (9th Cir. 1974). FTC's reliance on Tiversa to commence its inquisition, and its long defense of Tiversa notwithstanding Boback's evident perjury is precisely the kind of prosecutorial misconduct that violates LabMD's constitutional rights. *See Mesarosh v. United States*, 352 U.S. 1, 8-9 (1956); *Basurto*, 497 F.2d at 784; *Napue v. Illinois*, 360 U.S. 264, 269 (1959). FTC has, at a minimum, the duty to strip Boback's tainted testimony, and all derivative evidence (including expert opinions) from the administrative record. *Communist Party*, 351 U.S. at 125 (agency must base findings on untainted evidence and must expunge perjured testimony from the record).

Courts expect that federal lawyers with prosecutorial powers will treat targets of government investigations fairly by providing a "more candid picture of the facts and the legal principles governing the case." *See, e.g.*, James E. Moliterno, *The Federal Government Lawyer's Duty to Breach Confidentiality*, 14 Temp. Pol. & Civ. Rts. L. Rev. 633, 639 (2006).

"A government lawyer 'is the representative not of an ordinary party to a controversy,' the Supreme Court said long ago in a statement chiseled on the walls of the Justice Department, 'but of a sovereignty whose obligation ... is not that it shall win a case, but that justice shall be done.'" *Freeport-McMoran Oil & Gas Co. v. FERC*, 962 F.2d 45, 47-48 (D.C. Cir. 1992)(quoting *Berger v. United States*, 295 U.S. 78, 88 (1935)). Accordingly, "a government lawyer has obligations that might sometimes trump the desire to pound an opponent into submission." *Freeport-McMoran Oil & Gas Co.*, 962 F.2d at 48.

This heightened duty required first FTC and later Complaint Counsel to conduct a detailed and diligent investigation of Tiversa and the 1718 File before proceeding against LabMD. *See* 16 C.F.R. § 2.4 (stating that FTC's investigational policy mandates the "just . . . resolution of investigations"). Therefore, all of Complaint Counsel's evidence should be excluded as derivative of Tiversa's theft of the 1718 File and this case dismissed.

3. Kaloustian.

The exclusionary rule should prevent Complaint Counsel or its experts from using evidence obtained from the civil investigative deposition of Kurt Kaloustian. Kaloustian was compelled to give testimony pursuant to a FTC Civil Investigative Demand. The nonpublic proceeding took place on May 3, 2013 before FTC attorneys Laura Riposo VanDruff and Alain Sheer. Neither Kaloustian nor LabMD had counsel present. Prior to this hearing, on March 20, 2013, FTC was notified by LabMD that contacting former employees of LabMD was improper without first informing the company's legal counsel to properly preserve the attorney-client privilege. Yet LabMD was never told Kaloustian was to be deposed. Therefore, LabMD did not have counsel present and was not able to protect attorney-client privileged information.

Kaloustian's hearing was improper. *See* D.C. R. of Prof. Conduct 4.2; *Camden v. State of Maryland,* 910 F. Supp. 1115 (D. Md. 1996)(prohibiting *ex parte* contact with the former employee of a organizational party when the lawyer knows that the former employee was extensively exposed to privileged information). Therefore, Complaint Counsel should not be permitted to introduce his testimony and Complaint Counsel's experts' reliance on such testimony to form their opinions should be accorded very little if any evidentiary weight. [13]

4. Fair Process.

FTC owes LabMD a constitutional duty of impartiality free from the taint of bias, prejudice or pre-decision. FTC's misconduct and indiscretions, from case inception through the OGR investigation of Tiversa, and the statistical certainty that it will find a Section 5 violation *regardless of this Court's factual and legal findings,* breach this duty.

First, the Commission has violated LabMD's due process rights because in 2009, the FTC unlawfully modified its Rules of Practice to render motion practice functionally futile. 74 Fed. Reg. 20,205 (May 1, 2009). These modifications breached constitutional limits on blending of prosecutorial, legislative, and adjudicative functions, and wrongfully curtailed this Court's authority.

[13] Thus the following opinions of Dr. Hill for which she relies exclusively on the testimony of Kaloustian should be disregarded or accorded very little if any evidentiary weight:

- Penetration testing was never done. (CX 0740 (Hill, Rep. at 38)); (Hill, Tr. 276).
- Firewalls were disabled on servers that contained personal information. (CX 0740 (Hill, Rep. at 38)); (Hill Tr. 274-275).
- LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired in by Microsoft. (CX 0740 (Hill, Rep. at 42)).
- LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network. (CX 0740 (Hill, Rep. at 47)).
- Personal information was transmitted and stored in an unencrypted format. (CX 0740 (Hill, Rep. at 38)).

Second, the Commission has violated LabMD's due process rights because it is a statistical certainty that the Commission will find LabMD's data security practices are unfair under Section 5(n) no matter what this Court does. Nichole Durkin, *Rates of Dismissal in FTC Competition Cases from 1950–2011 and Integration of Decision Functions*, 81 Geo. Wash. L. Rev. 1684 (2013); *see also* Wright, *Recalibrating Section 5: A Response to the CPI Symposium*, CPI Antitrust Chronicle, November 2013 (in "100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed") https://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf. This clear inevitability of outcome transforms the adjudicatory process into punishment, forcing respondents with meritorious claims into a Hobson's choice between consent orders or spending huge sums defending against a preordained result. *See* Wright, "Section 5 Revisited: Time for the FTC to Define the Scope of Its Unfair Methods of Competition Authority," at 6 (Feb. 26, 2015) ("uncertainty surrounding the scope of Section 5 is exacerbated by the administrative procedures available to the Commission… in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ruled found no liability, the Commission reversed. *This is a strong sign of an unhealthy and biased institutional process*")(emphasis added), https://www.ftc.gov/system/files/documents/public_statements/626811/150226bh_section_5_symposium.pdf.

As the United States Supreme Court has stated:

> A fair trial in a fair tribunal is a basic requirement of due process. Fairness of course requires an absence of actual bias in the trial of cases. But our system of

> law has always endeavored to prevent even the probability of unfairness. To this end no man can be a judge in his own case and no man is permitted to try cases where he has an interest in the outcome.

In re Murchison, 349 U.S. 133, 136 (1953); *Gibson*, 411 U.S. at 578-79; *see also Marshall v. Jerrico, Inc.*, 446 U.S. 238, 242 (1980); *In the Matter of Dean Foods Co.*, 70 FTC 1146, 1966 FTC LEXIS 32 (1966) (fair hearing denied where a disinterested observer would have reason to believe that the Commission had in some measure adjudged the facts of a particular case in advance of hearing it). The Commission here has violated due process by the appearance of prejudgment.

There are two ways a plaintiff may establish that she has been denied her constitutional right to a fair hearing before an impartial tribunal. The proceedings and surrounding circumstances may demonstrate actual bias on the part of the adjudicator. *Taylor v. Hayes*, 418 U.S. 488, 501-04 (1974); *Cinderella Career and Finishing Schools, Inc. v. Federal Trade Comm'n*, 425 F.2d 583, 591 (D.C. Cir. 1970). Alternatively, the adjudicator's personal interest in the outcome of the proceedings may create an appearance of partiality that violates due process, even without any showing of actual bias. *Gibson*, 411 U.S. at 578; *Exxon Corp. v. Heinze*, 32 F.3d 1399, 1403 (9th Cir. 1994).

The surrounding circumstances demonstrate bias here. To begin with, the evidence of decades is the Commission will rule against LabMD no matter what this Court finds. Wright, *supra*. The facts suggest the Commission wrongfully used its enforcement authority to retaliate against LabMD for speaking out against government overreach. *See Trudeau v. Fed. Trade Comm'n*, 456 F.3d 178, 190-91, 190 n.22 (D.C. Cir. 2006) (official reprisal for constitutionally-protected speech violates the First Amendment).

Also, the circumstances suggest an appearance of partiality by the Commission against LabMD. The OGR investigation creates powerful institutional incentives for the Commission to prejudge this matter, because only a judgment against LabMD will rescue the Commission's reputation - any other result confirms government misconduct and creates potential civil liability. *Pillsbury Co. v. FTC*, 354 F.2d 952, 964 (1966)(litigant's right to a fair trial is breached where agency officials in judicial function are subjected to powerful external influences). Furthermore, the Commission has refused to comply with the Administrative Procedure Act provision governing *ex parte* contacts between it and Congress regarding matters relating to the facts and circumstances of this case. *See Aera Energy LLC v. Salazar*, 642 F.3d 212, 220-22 (D.C. Cir. 2011); 5 U.S.C. § 557(d)(1)(A); *see also United Steelworkers of Amer. v. Marshall,* 647 F.2d 1189, 1213 (D.C. Cir. 1980) (APA prohibits off-the-record communication between agency decision maker and any other person about a fact in issue); *see generally Pillsbury Co.*, 354 F.2d at 964. The only cure for such *ex parte* contact is full disclosure by Complaint Counsel of all *ex parte* communications and documents exchanged with Congress. 5 U.S.C. § 557(d)(1)(A). The Commission, however, has refused this clear directive. The Commission's refusal to disclose, when viewed in context of all the other facts and circumstances of this case, taints the proceeding with the appearance of bias.

D. APA Violations.

The Commission is bound by the Administrative Procedure Act ("APA").

To begin with, a consent decree is not binding authority or a legally-cognizable "standard" of agency expectations. *Altria Grp.*, 555 U.S. at 89 n.13; Rybnicek & Wright, *supra,* 21 Geo. Mason L. Rev. at 1305-06 ("[T]he Commission does not treat its settlements as

precedent, meaning that past decisions do not necessarily indicate how the agency will apply Section 5 in the future.").

General statements of policy are prospective and do not create obligations enforceable against third parties like LabMD. *See Am. Bus. Ass'n.*, 627 F.2d at 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a…policy statement announces the agency's tentative intentions for the future")(citation omitted); *Wilderness Soc'y*, 434 F.3d at 595-96. Therefore, if FTC truly considers "public statements," "educational materials," and "industry guidance pieces" to be enforceable standards or "statements of general policy," then it necessarily concedes an APA violation.

The APA requires agencies to "publish in the Federal Register for the guidance of the public…substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D). It further provides that except to the extent "that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published." 5 U.S.C. § 552(a)(1)(E). Therefore, internet postings of "Guides for Business," links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication. *Util. Solid Waste Activities Grp.*, 236 F.3d at 754.

The APA bars the Government from enforcing requirements it claims are set forth in the above-described materials absent Federal Register publication. *See* 5 U.S.C. § 552(a). As a matter of law, it obligates FTC to "separately state and currently publish in the Federal Register for the guidance of the public … *statements of general policy or interpretations of general*

applicability formulated and adopted by the agency…." *See* 5 U.S.C. § 552(a)(1)(D)(emphasis added). The APA bars agencies from enforcing statements of general policy and interpretations of general applicability "[e]xcept to the extent that a person has actual and timely notice" by Federal Register publication. *See* 5 U.S.C. § 552(a)(1)(E); *Util. Solid Waste Activities Grp.*, 236 F.3d at 754(internet notice is not an acceptable substitute for publication in the Federal Register).

15 U.S.C. § 57a(a)(1) authorizes the Commission to prescribe "interpretive rules and general statements of policy" with respect to unfair acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)(1)), and "rules" which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (within the meaning of § 45(a)(1)), except that the Commission shall not have authority to "develop or promulgate any trade rule or regulation with regard to the regulation of the development and utilization of the standards and certification activities pursuant to this section."

The Commission promulgates general statements of policy at 16 C.F.R. Part 14 but there is none for medical data security. The Commission promulgates guides for business but there are none for medical data security. *See, e.g.,*16 C.F.R. Part 251. The Commission promulgates trade rules for business but there are none for medical data security. *See, e.g.,* 16 C.F.R. Part 455.

The Commission cites as "standards" in this case materials that have not been published in the Federal Register in violation of 5 U.S.C. § 552(a)(1)(D). *See* Complaint Counsel's Pre-Trial Brief, *In the Matter of LabMD, Inc.*, FTC Dkt. 9357, at 13-14, 18-20 (May 6, 2014)(citations omitted). It has created and applied data security standards as if they had been promulgated as a guide or trade rule. *Compare* FTC, "Start With Security", https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (June, 2015); FTC, "Information Compromise and the Risk of Identity Theft: Guidance for Your

Business," https://www.ftc.gov/tips-advice/business-center/guidance/information-compromise-risk-identity-theft-guidance-your (June, 2004)(directing businesses to preferred contractors); 16 C.F.R. § 14.9 (titled "Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials" and warning "Any respondent who fails to comply with [the specified] requirement may be the subject of a civil penalty or other law enforcement proceeding for violating the terms of a Commission cease-and-desist order or rule"); 16 C.F.R. § 453.1 (funeral rule definitions).

The Commission's use of adjudication to set or apply supposedly preexisting medical data security standards that might add to or alter existing APA-promulgated HIPAA regulations or guidance, based on materials not previously published in the Federal Register is an abuse of discretion and contrary to law under the APA. 5 U.S.C. § 552(a)(1)(D)**.** FTC may proceed by adjudication only in cases where it is enforcing discrete violations of existing laws and where the effective scope of the impact of the case will be relatively small and by § 57a procedures if it seeks to change the law and establish rules of widespread application. *Ford Motor Co. v. FTC,* 673 F.2d 1008, 1010-11 (9th Cir. 1981).

Adjudication deals with what the law was; rulemaking deals with what the law will be. *Bowen v. Georgetown University Hospital*, 488 U.S. 204, 221 (1988)(Scalia, J., concurring)(citations omitted). The function of filling in the interstices of the FTC Act should be performed, as much as possible, "*through this quasi-legislative promulgation of rules to be applied in the future*.'" *See id.* (emphasis in original). As a matter of law, the Commission's adjudication is arbitrary and capricious. *Ford Motor,* 673 F.2d at 1010-11 (citation omitted).

Due to the communications between Congress and the Commission regarding this case, the APA required Complaint Counsel to place into the record all *ex parte* communications. *Aera*

Energy LLC, 642 F.3d at 220-22; 5 U.S.C. § 557(d)(1)(A); *see also United Steelworkers of Amer.*, 647 F.2d 1189, 1213 (D.C. Cir. 1980) (APA prohibits off-the-record communication between agency decision maker and any other person about a fact in issue); *Pillsbury Co.*, 354 F.2d at 964. Respondent filed motions regarding the disqualification of FTC commissioners on December 17, 2013, April 27, 2015, May 15, 2015, and July 15, 2015 which were wrongfully denied as a matter of law.

LabMD's business model offered groundbreaking benefits to doctors and patients, delivering pathology results to doctors electronically at unprecedented speed, allowing them to more quickly tell anxiously waiting patients whether they had cancer and to begin treatment immediately if needed. (Daugherty, Tr. 962) (A. "And in our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices. . . . the amount of errors just fell through the floor. . . . [W]e even knew ahead of time what was coming so that we could be prepared."). LabMD was mindful of its HIPAA obligations: It required doctors to use common authentication-related security measures. (RX 533 (Fisk, Rep. at 16-22)); (CX 0005 (LabMD Compliance Program)). However, FTC did not submit into evidence a reasoned countervailing benefit analysis as required by law. *Fox Television*, 556 U. S. at 515 (noting "the requirement that an agency provide reasoned explanation for its action").

If 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, then it violated the APA. *XP Vehicles, Inc. v. DOE*, 2015 U.S. Dist. LEXIS 90998, *94-100 (DDC 2015) (plaintiff alleging government

action taken against it for the benefit of government cronies, stated a claim for which relief could be granted).

II. Complaint Counsel Has Not Proven Its Case.

Even if Complaint Counsel could cure its many constitutional and statutory failings FTC should not prevail.

A. Complaint Counsel Does Not Meet Section 5(n).

Complaint Counsel has failed the statutory standard of proof, not by a preponderance of the evidence and certainly not by clear and convincing evidence.

- Complaint Counsel has failed to allege that LabMD's data security practices are "unfair" under Section 5(a) – that is, unjust, inequitable or designed to exploit and that the data security acts and practices identified in the Complaint are unfair to consumers generally and/or affected enough consumers to implicate or affect free and fair competition in the market generally. However, both are necessary elements. *Yates* 135 S. Ct. at 1081-83
- Complaint Counsel has failed to allege each challenged data security act or practice causes substantial injury now. This too is a necessary element. 15 U.S.C. § 45(n).
- Complaint Counsel has alleged LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks" and that these acts or practices are unfair and unlawful. Compl. at ¶¶ 10, 22. However, Section 5(n) limits the Commission's 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." It does not authorize the Commission to reach a "number of practices…taken together…." *See* 15 U.S.C. § 45(n).

- Complaint Counsel has failed to prove that LabMD's challenged data security acts and practices between January, 2005, and July, 2010, could reoccur and are likely to cause substantial consumer injury in the future as is required under 15 U.S.C. § 45(n). This is a necessary element of a *prima facie* case for past conduct, especially in a case without actual victims concerning acts or practices that ceased more than five years ago. However, Complaint Counsel has failed to prove it is "likely" (that is, it is highly or even merely probable) or that there is a legally cognizable danger that LabMD will engage in the supposedly unfair acts or practices in the future. *Borg-Warner Corp.*, 746 F.2d at 110-11; *W. T. Grant Co.*, 345 U.S. at 633.
- Complaint Counsel has failed to prove an actual data breach, which is necessary but not sufficient for a Section 5(n) violation. *See* 15 U.S.C. § 45(n); MTD Order at 18-19; *Wyndham Worldwide Corporation*, 10 F. Supp. 3d at 609; FTC Unfairness Statement (describing injury prong). The Complaint cites two "security incidents": The 1718 File and the Day Sheets. Complaint Counsel has abandoned the 1718 File.[14] As for the Day Sheets, this security incident is a fruit of the 1718 File and should be excluded on that

[14]Perhaps Complaint Counsel has at last recognized the perversity of its reliance on a corrupt and possibly criminal business to justify destroying an innovative cancer laboratory at the cost of five years of agency time and millions in taxpayer dollars. But Tiversa's/Privacy Institute's/FTC's grab of the 1718 File could not be legally cognizable evidence of injury, even if Complaint Counsel had not made its 11th hour concession and instead continued to stand with Tiversa. The evidence is that no consumer ever could likely be substantially harmed because the 1718 File never left Atlanta, Georgia, or "spread" across any P2P network and was only ever "found" by a uniquely skilled forensic computer analyst who was told to steal from innocent victims to "supplement" a propriety technology and to help his employer shake down victims using fabricated information. Other than this take by Tiversa, there is no evidence LabMD *ever* experienced a data breach.

basis alone. In any event, Complaint Counsel has not proven how the Day Sheets, each a paper record, were stolen from LabMD. According to Dr. Hill LabMD's physical security was "adequate." Therefore, Complaint Counsel has failed to prove substantial injury.

- Complaint Counsel must allege and prove by a preponderance of the evidence a consumer injury that is substantial, tangible and more than merely speculative. Established judicial principles help "ascertain whether a particular form of conduct does in fact tend to harm consumers." Speculation about possible identity theft and fraud does not satisfy Section 5(n)'s substantial injury requirement. *See* FTC Unfairness Statement; *compare Wyndham,* 10 F. Supp. 3d at 609. Established judicial principles suggest "substantial injury" under Section 5(n) must be more than an "injury in fact," that is, the invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). Yet Complaint Counsel has failed to show even this. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 47 F. Supp. 3d 27-33 (D.D.C. 2014) (listing cases).
- Complaint Counsel has failed to prove the potential injury in this case could not be mitigated after the fact. As the Ninth Circuit explained in *Davis v. HSBC Bank Nevada*, an "injury" is not actionable under Section 5(n) "if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." 691 F.3d 1152, 1168-69 (9th Cir. 2012). *Davis* rejected the notion that avoiding injury is itself sufficient, framing the issue as "not whether subsequent mitigation was convenient or costless, but whether it was reasonably possible." *Id.*

- Complaint Counsel has failed to allege or prove by a preponderance of the evidence that the substantial consumer injury in this case is widespread or that the acts or practices at issue here were unfair to the public generally.
- FTC has bound Complaint Counsel to its Unfairness Statement, which requires some connection between an alleged unfairness and some form of LabMD behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making to determine substantiality. *See* Beales, *supra*. Yet Complaint Counsel has not alleged or proven that LabMD has unreasonably created or taken advantage of any such obstacles. Therefore it has failed to establish "substantiality."
- Complaint Counsel has failed to prove that the substantial consumer injury FTC believes LabMD's data security acts and practices between January, 2005, and July, 2010, is likely to cause in 2015 and beyond is not outweighed by countervailing benefits to consumers or to competition.
- Complaint Counsel has not alleged or proven LabMD unreasonably relied on its IT experts. *Fabi Constr. Co.*, 508 F.3d at 1084.
- Complaint Counsel's position is "The enforcement of OSHA's General Duty Clause in Department of Labor administrative courts may provide the best analogy to a data security administrative hearing under Section 5 of the FTC Act. *See, e.g.*, *Fabi Constr. Co.*, 508 F.3d at 1088 (considering a number of factors to determine whether defendant met its 'general duty,' including whether defendant followed third-party technical drawings, whether defendant complied with industry standards, and expert opinion)." Complaint Counsel's Response In Opposition to Respondent's Motion to Dismiss Complaint In the Matter of LabMD, Inc., FTC Dkt No. 9357 at 19, fn. 12. (Nov. 22,

2013). Section 5(n), not the OSHA General Duty Clause, controls here. *Compare* 15 U.S.C. § 45(n); 29 U.S.C. § 654(a) ("Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees [and] shall comply with occupational safety and health standards promulgated under this chapter.") But if this Court adopts Complaint Counsel's proffered approach, then it must apply terms consistently. In General Duty Clause cases, "industry standards" are concrete and discernible standards applicable to a given company in its particular line of business. *See Fabi Constr. Co.*, 508 F.3d at 1084 (industry standards for a building construction company applied); *Ensign-Bickford Co. v. OSHRC*, 717 F.2d 1419, 1422 (D.C. Cir. 1983)(industry standards for the pyrotechnic industry applied); *S&H Riggers*, 659 F.2d at 1280-83 (reasonable-person standard divorced from relevant industry standards or regulations violates due process). Here, that means medical industry standards.[15] Complaint Counsel has not alleged or proven LabMD breached applicable medical industry standards during the relevant time.

Section 5(n) requires Complaint Counsel to prove that a challenged act or practice is "likely" (probable) to cause "substantial injury" to consumers that is not reasonably avoidable by them or outweighed by countervailing benefits. 15 U.S.C. § 45(n). "The Commission is not concerned with trivial or merely speculative harms." Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in Int'l Harvester Co*.,

[15]Industry standards and customs are not entirely determinative of reasonableness because there may be instances where a whole industry has been negligent. However, such negligence on the part of a whole industry cannot be lightly presumed. *Diebold, Inc. v. Marshall*, 585 F.2d 1327 (6th Cir. 1978). It must be proven and Complaint Counsel has not done so, meaning medical industry standards must apply here.

104 F.T.C. 949, 1984 FTC LEXIS 2, at *308-09 (1984) (emphasis added); *accord Reilly v. Ceridian Corp.*, 664 F.3d 38, 44-46 (3rd Cir. 2011); Beales, *supra* (unfairness authority aimed at "*widespread and significant consumer harm*") (emphasis added).

FTC's Unfairness Statement provides "[i]n most cases a substantial injury involves monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction." https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (last visited August 9, 2015). Complaint Counsel must allege and prove by a preponderance of the evidence that the allegedly unfair and unlawful data security acts and practices identified in the Complaint to cause substantial consumer injury are unfair to consumers generally and/or affected enough consumers to implicate or affect free and fair competition in the market generally. 16 C.F.R. § 3.43; 15 U.S.C. §§ 45(a), (n); *American Bldg. Maintenance Indus.*, 422 U.S. at 277; *Yates*, 135 S. Ct. at 1085, 91; Beales, *supra* (unfairness authority is "a powerful tool for the Commission" to attack a particular Respondent's practices "that may not involve deception but nonetheless cause *widespread and significant consumer harm*")(emphasis added).

Established judicial principles help FTC "ascertain whether a particular form of conduct does in fact tend to harm consumers." *Int'l Harvester Co.*, 1984 FTC LEXIS 2, at *313 (citation omitted). To prove "substantial injury" in this case as a matter of law, Complaint Counsel must first prove *both* actual data breaches *and* that LabMD's data security practices were "unreasonable" for medical companies during the relevant time frame. *See* 15 U.S.C. § 45(n); MTD Order at 18; *Fabi Const. Co.*, 508 F.3d at 1088 (industry standards for building construction company applied); *Ensign-Bickford Co.*, 717 F.2d at 1422 (industry standards for

pyrotechnic industry applied); *S&H Riggers*, 659 F.2d at 1280-83(reasonable-person standard divorced from relevant industry standards or regulations violates due process).

Proof of an actual data breach is a necessary but not sufficient condition for "substantial injury" as a matter of law under Section 5(n). According to the Commission:

> Notably, the Complaint's allegations that LabMD's data security failures led to actual security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in 'unfair . . . acts or practices'….the mere fact that data breaches actually occurred is not sufficient to show a company failed to have reasonable "we will need to determine whether the 'substantial injury' element is satisfied by considering not only whether the facts [of actual data breaches] alleged in the Complaint actually occurred but also whether LabMD's data security procedures were 'reasonable' in light of the circumstances.

MTD Order at 18-19 (citations omitted); *compare Wyndham*, 10 F. Supp. 3d at 609 (FTC alleged three actual data breaches leading to "the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm").

Complaint Counsel has failed to prove by a preponderance of the evidence that either of the Security Incidents alleged in the Complaint constituted an actual data breach. *See* MTD Order at 18-19; *Wyndham*, 10 F. Supp. 3d at 609. Speculation about possible identity theft and fraud does not satisfy Section 5(n)'s substantial injury requirement as a matter of law. *Reilly*, 664 F.3d at 44-46; *compare Wyndham*, 10 F. Supp. 3d at 609.

Established judicial principles suggest "substantial injury" under Section 5(n) must at least be more than an "injury in fact," that is, the invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. *Lujan*, 504 U.S. at 560 (1992). While the test for constitutional standing is low, *see, e.g.*, *Blunt v. Lower Marion Sch. Dist*., 767 F.3d 247, 278 (3rd Cir. 2014) (requiring only "some specific, identifiable trifle of injury"), Section 5(n) contains two additional requirements: the injury must be (1) "substantial," which, to have any meaning, must be something more than the injury required by Article III; and, (2) not "reasonably avoidable by consumers themselves." 15 U.S.C. § 45(n).

In data breach cases where no misuse is proven there has been no injury as a matter of law. *Reilly*, 664 F.3d at 44. An "injury" is not actionable under Section 5(n) "if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." *Davis*, 691 F.3d at 1168-69. The issue "not whether subsequent mitigation was convenient or costless, but whether it was reasonably possible." *Id.* at 1169. As a matter of law, speculation about the potential time and money consumers could spend resolving fraudulent charges cannot satisfy Section 5(n), or even confer standing under Article III. *See id.; Reilly*, 664 F.3d at 46 (alleged time and money expenditures to monitor financial information do not establish standing, "because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than alleged 'increased risk of injury' claims"); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007) ("lost data" cases "clearly reject the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring his or her credit"). That a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a "concrete and particularized" or "actual or imminent" injury. *In re Sci. Applications Int'l Corp.*

(SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28-33 (D.D.C. May 9, 2014) (listing cases).

B. FTC Expert Opinions

In addition to Complaint Counsel's failure to make a prima facie case against LabMD, Complaint Counsel expert opinions should be deemed inadmissible or given very little weight because they lack scientific and factual credibility. Thus, FTC is unable establish that LabMD's data security practices were unfair pursuant to Section 5(n). Consequently, Complaint Counsel's case is built on irrelevant and/or unreliable expert testimony that should be excluded or given little or no weight. *See Daubert v. Merrell Dow Pharmacuticals*, 509 U.S. 579 (1993); *AG of Okla. v. Tyson Foods, Inc*., 565 F.3d 769, 780 (10th Cir. 2009); *In re McWane, Inc.*, 2012 FTC LEXIS 142, at *8 (Aug. 16, 2012)(citations omitted).[16]

FTC affirmatively lacks objective data security standards for the medical industry or anyone else. *See* (RX 0526) (none of the documents available on the Internet on the FTC's 'Bureau of Consumer Protection Business Center's' self-described 'Legal Resources' website, including but not limited to consent orders and FTC 'Guides for Business,' establish specific data-security practices which any U.S. company must adopt to comply with 15 U.S.C. § 45(a),(n)).

Complaint Counsel proffers the expert opinions of Dr. Raquel Hill, Jim Van Dyke, and Richard Kam to substantiate their claims that LabMD's data security practices should be

[16]To be qualified an expert must have relevant "knowledge, skill, experience, training, or education." *See* Fed. R. Evid. 702. To be reliable, an expert's methodology must pass muster under the following factors: (1) whether the expert's theory can be and has been tested; (2) whether the theory has been subjected to peer-review and publication; (3) the known or potential rate of error of the particular scientific technique; and (4) whether the technique is generally accepted in the scientific community. *See Daubert*, 509 U.S. at 593-94; *Kilpatrick v. Breg, Inc*., 613 F.3d 1329, 1335 (11th Cir. 2010).

declared unlawful, upon a finding that its practices were unfair pursuant to Section 5(n). Dr. Hill offered an opinion concerning the adequacy of LabMD's data security, while both Jim Van Dyke and Richard Kam opined about the likelihood that LabMD's data security practices will cause substantial consumer injury. However, as explained below, each expert opinion suffers the same fate – their opinions should be accorded little if any weight.[17]

Because Complaint Counsel's case is devoid of any admissible or credible expert opinions, they are unable establish that LabMD's data security practices were unfair.

1. Dr. Hill's expert opinion should be accorded no weight.

Dr. Raquel Hill is a professor of Computer Science at Indiana University, and was engaged by the FTC to "assess whether LabMD provided reasonable and appropriate security for Personal Information within its computer network." (CX 0740 (Hill, Rep. at 3)). Dr. Hill opined that between January 2005 and July 2010 "LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures." (CX 0740 (Hill, Rep. at 20)). Hill further opined that "LabMD did not develop, implement or maintain a comprehensive information security program to protect consumer's Personal Information." (CX 0740 (Hill, Rep. at 24)). According to Dr. Hill, maintaining a comprehensive information security program includes employing a defense in depth strategy, which in turn includes addressing the seven principles she outlines in her report. (CX 0740 (Hill, Tr. 307-309)). As explained below, Dr. Hill's opinion should be accorded little or no weight.

[17] Respondent renews, as fully incorporated herein, its oral and written Daubert motions regarding each of the experts. *See* (Hill, Tr. 325-330); (Van Dyke, Tr. 741-744); Respondent's Motion in Limine to Exclude Expert Testimony of James van Dyke, dated April 22, 2014; (Kam, Tr. 569-573); Respondent's Motion in Limine to Exclude Expert Testimony of Richard Kam, dated Apr. 22, 2014).

i. **Dr. Hill's seven principles for assessing and securing a network are unreliable, and thus her opinion should be accorded little or no weight.**

Dr. Hill states that "[t]here are seven principles that help specify the policies and identify the mechanisms that are to be deployed at each layer of a defense in depth security strategy." (CX 0740 (Hill, Rep. at 14)). The seven principles are: (1) Don't keep what you don't need, (2) Patch, (3) Ports, (4) Policies, (5) Protect, (6) Probe, and (7) Physical. (CX 0740 (Hill, Rep. at 13-15)). However, besides her report, Dr. Hill is unaware of any document that cites there are "seven principles for a comprehensive information security program." (Hill, Tr. 242-243). Let alone, no evidence in the record suggests that these seven principles have been subject to testing or peer review. For this reason, Dr. Hill's should be accorded little or no weight.

ii. **Dr. Hill's opinion fails to consider medical industry standards in effect and applicable to businesses of LabMD's size and nature contrary to *S.H. Riggers*, and thus should be accorded little or no weight.**

A reoccurring issue in this case has been whether LabMD is responsible for complying with data security standards followed in the general Information Technology industry, or data security standards followed in the medical industry. *S&H Riggers* makes clear that the latter should be followed. *S&H Riggers & Erectors*, 659 F.2d at 1280-83 (reasonable-person standard divorced from industry standards or regulations violates due process). Dr. Hill opines on data security standards relating to the general Information Technology industry. (Hill, Tr. 234);(CX 0524 (Hill, Dep. at 61)). In contravention of *S&H Riggers*, Dr. Hill's opinion failed to take into account objective medical industry standards in effect and applicable to businesses of LabMD's size and nature. In fact, Dr. Hill admits that she has never worked for a medical provider or lab. (CX 0524 (Hill, Dep. at 150)). Thus, Dr. Hill's opinion should be accorded little or no weight.

iii. **By relying on the "defense in depth" strategy, Dr. Hill's opinion fails to set forth a data security standard that LabMD would have had notice of during the Relevant Time Frame, and thus her opinion should be accorded little or no weight.**

Dr. Hill's opinion "covers the time period from January 2005 through July 2010," which further states that "[t]he most effective way to secure a network and its computers is by using multiple security measures to provide defense in depth" (CX 0740 (Hill, Rep. at 3, 10)). Indeed, Dr. Hill considers it necessary for a company to employ "defense in depth" in order to exercise reasonable care. (Hill, Tr. 306-310). As such, much of Dr. Hill's opinion and trial testimony is devoted to whether LabMD deployed a defense in depth approach when securing its data.

Interestingly, Dr. Hill only became aware of the defense in depth strategy circa mid-2009. (Hill Tr. 306)("I think it was maybe around five years ago or so when I became familiar with the strategy."). Thus, application of Dr. Hill's opinion to the instant matter would require LabMD to have known about and complied with the defense in depth standard beginning in January 2005 – three and half years before Dr. Hill was even aware that the "defense in depth" strategy existed. Surely, LabMD should not be held accountable for implementing a strategy that the FTC's expert was not even aware existed. For this reason, Dr. Hill's opinion should be accorded little or no weight.

iv. **Dr. Hill relies heavily on unreliable information from Curt Kaloustian and Robert Boback to support factual bases of her opinion, and thus her opinion should be accorded little or no weight.**

Dr. Hill relies only on factual information from Curt Kaloustian's Investigational Hearing Transcript to conclude that:

- Penetration testing was never done. (CX 0740 (Hill, Rep. at 38)); (Hill, Tr. 276).
- Firewalls were disabled on servers that contained personal information. (CX 0740 (Hill, Rep. at 38)); (Hill Tr. 274-275).

- Personal information was transmitted and stored in an encrypted format. (CX 0740 (Hill, Rep. at 38)).
- LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired in by Microsoft. (CX 0740 (Hill, Rep. at 42)).
- LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network. (CX 0740 (Hill, Rep. at 47)).

LabMD was not made aware that Complaint Counsel was taking Curt Kaloustian's investigational hearing deposition, and thus was unable to cross-examine Kaloustian. In addressing this precise matter, this court said " . . .[investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding." Final Prehearing Conference, dated May 15, 2014, at 9-10. Here, the above-mentioned portions of Dr. Hill's report that relies on uncross-examined testimony should be accorded no weight.

Moreover, Dr. Hill also relies on information from Robert Boback and Tiversa to conclude that "[c]opies of the 1718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom." (CX 740 (Hill, Rep. at 17)). This fact was shown to be patently false. Richard Wallace testified that the 1718 File never spread anywhere on the internet, and that Tiversa created and maintained this lie to retaliate against LabMD. (Wallace, Tr. 1367-1370). This portion of Dr. Hill's opinion should be accorded little or no weight.

v. **Dr. Hill failed to consider the FTC's standards and guidelines in formulating her opinion whether LabMD's data security was reasonable, and thus her opinion should be accorded little or no weight.**

The crux of this case boils down to whether LabMD provided adequate data security for PHI stored on its network. And the FTC has maintained that LabMD should have not only complied with Section 5(n), but also that it should have complied with the FTC's widely available and known standards and guidelines regarding data security. (RX 525 (Kaufman, Dep. at 190, 207-210)). Interestingly, Dr. Hill admits that in her rendering her expert opinion that LabMD's data security was insufficient, she does not cite to any of these purportedly widely available and known FTC standards and guidelines. (Hill, Tr. 230-23; 240-241). Because Dr. Hill failed to apply the FTC's purported standard and guidelines to assess whether LabMD implemented adequate data security, her opinion should be accorded little or no weight.

"The rule is, a witness who's an expert is limited to opinions contained in the expert report that is vetted properly through discovery....". (ALJ Chappell, Tr. 513-514). Dr. Hill was not asked and did not opine regarding LabMD's current data security practices or whether those practices now cause substantial consumer injury and are unreasonable. Dr. Hill was not asked and did not opine whether the allegedly unreasonable LabMD's data security practices during the 2005-2010 time-frame are "likely" or probable to reoccur, and if so, to cause harm in the future. When asked if she had an opinion with respect to harm Hill rsponded that she assumed harm and therefore did not form an opinion in that regard:

> Q. [Mr. Sherman] So it's fair to say then that you have no opinion with regard to the likelihood of harm because it was assumed in your report; correct?
>
> A. [Ms. Hill] I have no opinion, yes.

(Hill, Tr. 218).

vi. Dr. Hill's testimony does not fit this case.

An expert's testimony must "fit" the case at hand. For example, the testimony of a chemistry expert that a ladder had a manufacturing defect because of a lack of adhesion between

its chemical components did not fit the facts of the case because the legal standard for a manufacturing defect was whether the product deviated in a material way from the industry's manufacturing specifications, and the expert did not assess whether the ladder met those standards. *See Leverette v. Louisville Ladder Co*., 183 F.3d 339, 341 (5th Cir. 1999). Dr. Hill's opinion does not "fit" this case for she evaluated LabMD's data security using broad, general IT principles from 2014 and without reference to or apparent knowledge of medical industry standards and practices during the relevant time.

For example, she considered only the HIPAA security rule but did not consider the rest of the statutory or regulatory HIPAA/HITECH data-security regime or perform the "scalability" analysis HIPAA requires to differentiate between large and small medical providers. (Hill, Tr. 246); Respondent LabMD's Proposed Findings of Fact, at I.J.2.a.vii(1). This was a major defect in her analysis: "Scalability" is a key tenet of HIPAA's security standard, providing that data security compliance must be judged according to the size and nature of the medical provider in question. *See* 68 Fed. Reg. 8335, 38-49, 51, 59-64, 67-69, 72-73; 45 CFR Parts 160, 162, 164.

2. Jim Van Dyke's expert opinion should be accorded little or no weight.

Jim Van Dyke is the founder and President of Javelin Strategy & Research and was engaged by the FTC to "assess the risk of injury to consumers whose personally identifiable information has been disclosed by LabMD, Inc without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure." (CX 0741 (Van Dyke, Rep. at 2)). In rendering his expert opinion, Van Dyke assumed that "LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks." (CX 0741 (Van Dyke, Rep. at 2)). Specifically, Van Dyke also assumed that the "1718 File and the day sheets were found outside

of LabMD as a result of a data breach." (Van Dyke, Tr. 678-679). Relying on a 2013 survey that Van Dyke's company Van Dyke ultimately concluded that:

> It is my opinion that LabMD's failure to provide reasonable and appropriate security for [the 1718 File, Day Sheets, and personally identifiable information maintained on LabMD's computer network] places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of what is commonly called "identity theft . . .

(CX 0741 (Van Dyke, Rep. at 3)).

i. **Van Dyke's opinions are not sufficiently connected to the facts of this case, and thus his opinion should be accorded little or no weight.**

"[T]estimony that is insufficiently connected to the facts of the case can serve as grounds for rejection of expert testimony." *Arista Records LLC v. Lime Group LLC*, No. 06-CV-5936-KMW, 2011 U.S. Dist. LEXIS 47416, *13 (S.D.N.Y. Apr. 29, 2011). In this case, Van Dyke's analysis is wholly disconnected from the facts of the case which renders his opinions unreliable. *See* (RX 523 (Van Dyke, Dep. at 39))(testifies that he "hadn't given any consideration" to how the insurance aging file was taken). Van Dyke's open admission that he never considered any of the specific facts of the case, (CX 741 72-73), illustrates that Van Dyke's opinions are speculative and unreliable. *Brooks v. Outboard Marine Corp.*, 234 F.3d 89 (2nd Cir. 2000) (upholding the trial court's decision to exclude a liability expert's opinion as unreliable as, among other shortcomings, he did not know "precisely what happened" during the accident which caused the plaintiff's injury).

Mr. Van Dyke has testified that he did not consider many of the different facts of this case in arriving at his report conclusions, leaving many holes in his report. Perhaps most surprisingly, Mr. Van Dyke's analysis did not account for type of breach or who gained the information. (RX 523 (Van Dyke, Dep. at 43, 58)). For example, it would make sense that the data being found on the IP address of an identity thief would have a higher risk of damage than if

the data was found on the IP address of Tiversa. However, Mr. Van Dyke's analysis did not incorporate different types of breach by different actors as factors relevant to likely injury.

Moreover, his analysis failed to include any temporal component, and assumed that the same amount of damage would occur from the disclosure of the information regardless of whether it was available for twelve months or four years. (RX 523 (Van Dyke, Dep. at 41)). The entire premise of Mr. Van Dyke's conclusion that consumers will be harmed rests solely on a question in survey performed in 2013 which measures the rates of identity fraud among people who had been notified within the last 12 months (of taking the survey) that their personal or financial information had been lost, stolen, or compromised in a data breach. (Van Dyke, Tr. 657). Data collection for this survey took place from October 9 to October 2013. (CX 0741(Van Dyke, Rep. at 4)). Thus, those responding to this survey question are responding that they were notified some time post October 9, 2012 that they were notified that their personal or financial information had been lost, stolen, or compromised in a data breach. This study is inapposite to the instant matter because the insurance aging file escaped LabMD's possession in 2008, some five years before the survey. In order for the results of the survey to have any relevance to the matter at hand it seems that the consumers listed on the 1718 file would have had to have participated in the survey and they would have needed to have been notified that their information had been lost stolen or compromised in a data breach within twelve months of taking the survey.

Van Dyke ultimately concluded that based on the survey, he would have expected to see *over two-thousand five-hundred* cases of identity fraud based on disclosure of the 1718 file, and over *one hundred and sixty cases* of identity fraud based on the disclosure of the Day Sheets within a twelve month period of notification. (CX 0741 (Van Dyke, Rep. at 12). In Van Dyke's

survey that event is notice from a financial institution, (RX 523 (Van Dyke, Dep. at 51)); here upon cross examination the event becomes twelve months after Boback's false testimony that the file was found in November of 2013. (RX 523 (Van Dyke, Dep. at 106-107)). The fact that no evidence of a single consumer becoming a victim of identity fraud because of disclosure of the 1718 file or the Day Sheets should cast doubts on the reliability of Van Dyke's survey, report and ultimately his expert opinion. For this reason, Van Dyke's report should be accorded little or no weight. *See EEOC v. Freeman*, 778 F.3d 463, 466, 469 (4th Cir. 2015)(citations omitted).

3. Richard Kam's expert opinion should be accorded little or no weight.

i. Kam utilized an unreliable four-factor methodology to evaluate the risk of medical identity theft related to the 1718 File and Day Sheet disclosures, and thus his opinion should accorded little or no weight.

Kam invented a four-factor methodology for evaluating the risk of harm from data breaches and applied it to this case. Kam's four factors include: (1) the nature and extent of the sensitive personal information involved, (2) the unauthorized person who used the protected health information or to whom the disclosure was made, (3) whether the sensitive personal information was actually acquired or viewed, and (4) the extent to which the risk to the protected health information has been mitigated. (CX 0742 (Kam, Rep. at 18)). However, Kam's test has not been peer reviewed or published, nor has it been used by other experts in the industry. And as Kam testified, he has never published his test and all of his prior applications of the test are cloaked by confidentiality agreements. (RX 522 (Kam, Dep. at 46-47)). Kam admitted that he did not consult a single academic paper or statistical survey in formulating the factors of his test. (RX 522 (Kam, Dep. at 45-46)) In *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 157 (1999), the Supreme Court upheld the exclusion of the expert's testimony because it "found no indication in the record that other experts in the industry use" the expert's test, or that experts in the industry

normally make the kinds of judgments "that were necessary, on [the expert's] own theory, to support his conclusions," or that the record contained reference to "any articles or papers that validate [the expert's] approach." Similar to the expert in *Kumho*, Richard Kam's expert opinion should be accorded little or no weight. *Accord Freeman,* 778 F.3d at 466.

ii. Even if this Court finds that Kam's four-factor methodology applies, his analysis of the 1718 File is not sufficiently connected to the facts of this case and thus his opinion should be accorded little or no weight.

Kam's analysis of the second, third, and fourth prongs of his self-invented methodology are unreliable. Prongs two and three consider to whom the 1718 File was disclosed and that the file was acquired and viewed. Prong four considers the extent to which disclosure was mitigated. Kam relied on Robert Boback's testimony to conclude that the 1718 File was found on four IP addresses, and was available as late as November 21, 2013 on the peer to peer network. Moreover, Boback stated that the 1718 was "available to anyone who had access to a peer-to-peer network." (CX 0742 (Kam, Rep. at 19)). However, testimony from Wallace reveals that the 1718 File was never found on the four IP addresses that Boback asserts, and that the file is not available. (Wallace, Tr. 1367-1370). Thus, there is no credible evidence in the record that the 1718 File was disclosed or acquired as stated by Boback, and relied on by Kam. Because of Robert Boback's perjured testimony, Complaint Counsel does not intend to cite to expert conclusions predicated on CX 0019 or Mr. Boback's testimony. *See* Complaint Counsel's Opp. to Mot. to Admit Select Exhibits, FTC Dkt. No. 9357 at 10-11 n.11 (June 24, 2015). Without reliance on Boback's testimony, prongs two, three and four of Kam's flawed four-factor test cannot be established. Thus, Kam's expert opinion should be accorded little or no weight.

iii. Also, Kam's analysis of the Day Sheet Incident is erroneous, and thus his opinion should be accorded little or no weight.

Under the second prong of Kam's four-factor methodology, he assesses to whom the Day Sheets were disclosed. However, Kam made the false assumption that the suspects in whose Sacramento house LabMD's Day Sheets were found had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012," when in fact they did not. (RX 522 (Kam, Dep. at 147-148). Kam's opinion regarding consumer harm from the Day Sheets is unreliable and irrelevant, and thus should be accorded little or no weight.

Moreover, Kam's analysis of the likelihood of harm from the disclosure of social security numbers in the Day Sheets was premised on the purported social security numbers in the CLEAR database, which have been excluded from the case by this Court as unreliable. (CX 0742 (Kam, Rep. at 23)); (Wilmer, Tr. 372). Therefore, Kam's entire analysis of the social security numbers no longer has any reliable factual basis in this case.

iv. Kam cannot explain why, contrary to his estimation, no consumer has reported becoming a victim of medical fraud due to the disclosure of the 1718 File.

Kam estimated that there would be 76 victims of medical identity theft due to the alleged disclosure of the 1718 File. (CX 0742 (Kam, Rep. at 19)). Kam is unable to reconcile this estimation with the fact that the record reflects that no victims of medical fraud have been identified. Kam stated that in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532). However, Kam admitted that his expert opinion did not account for the absence of any evidence of victims in this case. (Kam Tr. 532). For this reason, Kam's expert opinion should be deemed inadmissible, or alternatively accorded little or no weight.

v. Kam's claims that consumers were likely to incur emotional or subjective harm are not cognizable under section 5

Kam repeatedly mentions the possibility of embarrassment, specifically from the alleged exposure of CPT codes, which indicate that a person has paid for a particular laboratory test to be run. (CX 0742 (Kam, Rep. at 16, 21)). Kam acknowledges that CPT codes indicate only that testing has been paid for, and do not "indicate a diagnosis." (CX 0742 (Kam, Rep. at 16)). But, he goes on to claim that "disclosure of the fact that the tests were performed could cause embarrassment or other negative outcomes, including reputational harm" without explaining how likely it is that a person "could" be embarrassed or suffer reputational harm from the mere fact that a medical test had been paid for. (CX 742 (Kam, Rep. at 16)). However, even if Kam could establish a connection between CPT codes and "embarrassment" or reputational impact, it would be irrelevant—because embarrassment or reputational impact is an "emotional" or "subjective" harm, it is not cognizable as "substantial injury" under Section 5. Emotional harm such as embarrassment or reputational impact does not constitute "substantial injury" under Section 5. Substantial injury generally involves monetary harm, but "[e]motional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair." *See* FTC's Unfairness Statement. Therefore, Kam's testimony about this type of harm is not relevant to the facts of this case, and his opinion should be accorded little or no weight.

Boback stated that the 1718 was "available to anyone who had access to a peer-to-peer network." However, testimony from Wallace reveals that the 1718 File was never found on the four IP addresses that Boback asserts, and that the file is not available. Thus, there is no credible evidence in the record that that the 1718 File was disclosed or acquired as stated by Boback, and relied on by Kam. Because of Robert Boback's perjured testimony, Complaint Counsel does not intend to cite to expert conclusions predicated on CX 0019 or Mr. Boback's testimony. *See*

Complaint Counsel's Opp. to Mot. to Admit Select Exhibits at 10-11 n.11 (June 24, 2015). Without reliance on Bobcak's testimony, prongs two, three and four of Kam's flawed four-factor test cannot be established. Thus, Kam's expert opinion should be deemed inadmissible, or alternatively accorded little or no weight.

Moreover, Kam's analysis of the likelihood of harm from the disclosure of social security numbers in the Day Sheets was premised on the purported social security numbers in the CLEAR database, which have been excluded from the case by this Court as unreliable. Kam Report Wilmer Tr. 372, Therefore, Kam's entire analysis of the social security numbers no longer has any reliable factual basis in this case.

C. Proof failures.

Complaint Counsel has not proven LabMD's data security acts or practices between January, 2005, and July, 2010, now cause, or are likely to reoccur and likely to cause in the future, substantial consumer injury which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. *See* 15 U.S.C. § 45(n).

Complaint Counsel has not proven an actual data breach involving consumers as the Commission requires. *See* MTD Order at 18-19.

Complaint Counsel has not proven LabMD's data security practices violated a "reasonableness" standard that cannot be construed in a way that violates LabMD's due process rights.

1. Knowledge of standards.

To begin with, Complaint Counsel has not alleged, much less proven, that LabMD knew or should have known FTC expected PHI data security measures not required by HHS, but failed

to comply. *See S&H Riggers*, 659 F.2d at 1285. Instead the FTC accuses LabMD only of having violated a varying, subjective reasonableness standard—which it analogized to a negligence or "prudent person," standard of care—not present in Section 5. *See, e.g.*, Complaint Counsel's Pre-Trial Brief, *In the Matter of LabMD*, Dkt. No. 9357, at 19-22 (May 6, 2014).

Complaint Counsel asserts a "reasonableness" standard applies, but nowhere has FTC articulated a "reasonableness" standard applicable to this case, this respondent, or this industry. *See, e.g.*, Complaint Counsel's Pre-Trial Brief, *In the Matter of LabMD*, Dkt. No. 9357, at 16-21 (May 6, 2014) ("Legal Standard Under Section 5: Reasonable Security . . . [W]hat constitutes reasonable data security practices . . . will vary depending on the circumstances.").

Due process required FTC to articulate and apply an objective and industry-specific "reasonableness" standard of care to LabMD *ex ante* and Complaint Counsel has not met its burden in this respect. There is no evidence the data security program described by Dr. Hill was actually used by any medical provider during the relevant time or today.

2. Boback/Tiversa.

This case was commenced and prosecuted in reliance on perjured and falsified testimony from Tiversa and Boback.

Complaint Counsel entirely relies on the expert report and testimony of Dr. Hill to make a *prima facie* case. However, Dr. Hill's expert report (written by someone who never worked for a health care provider or in the health care industry, and therefore fails the test of *S&H Riggers*, 659 F.2d at 1280-83) assumes the 1718 File proliferated to four IP addresses outside of Atlanta, Georgia and is predicated on perjured testimony. (CX 0740 (Hill, Rep. at 15, 17-18)); (CX0741 (Van Dyke, Rep. at 2, 4, 7-8)); (CX 0742 Kam, Rep. at 6, 9, 18-19)); (CX 0738 Shields, Rep. at 3, 25)).

3. Substantial injury.

Complaint Counsel has failed to prove that LabMD's data security practices between 2005 and 2010 caused substantial injury to a single consumer. Merely speculative harm is not "substantial injury" under Section 5(n). Van Dyke and Kam (to the extent their opinions have any weight) only speculate about harm for there are no victims in this case.

Complaint Counsel also has failed to prove LabMD's data security practices, as they existed between 2005 and 2010, are likely reoccur and to cause substantial injury to consumers. In any event,

Complaint Counsel has also failed to prove the benefit, in terms of reduced risk from changing LabMD's data-security practices would have outweighed not only the costs to LabMD but also the additional burdens to the doctors and their patients who benefitted from the potentially life-saving speed and accuracy of LabMD's system. *See* LabMD's Proposed Findings of Fact; (Daugherty, Tr. 962, 959-960). Dr. Hill certainly could not testify to this – she knew nothing of LabMD's business or the medical industry generally.

Complaint Counsel must prove LabMD's data security practices were likely to cause substantial injury "which is not reasonably avoidable by consumers themselves." *See* 15 U.S.C. § 45(n). The law is "Consumers may act to avoid injury before it occurs if they have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end." *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988).

Other than Tiversa, Johnson, and FTC, no person had the 1718 File. Complaint Counsel has not proven that these persons threatened to steal consumers' identities or commit financial fraud. As for the Day Sheets, Complaint Counsel has failed to prove by a preponderance of the

evidence that the consumers affected by the Sacramento incident could not reasonably avoid the risk of harm , and therefore Complaint Counsel cannot show that LabMD violated Section 5(n) with respect thereto. The two suspects in Sacramento had no connection to LabMD and were never charged with any crime due to their possession of the Day Sheets.

In truth, FTC delayed LabMD's response to the Day Sheet incident. On January 30, 2013, the FTC informed LabMD that the Day Sheets had been discovered in Sacramento. LabMD tried to investigate what information might have been at risk in order to provide fuller and more useful notice, but the FTC refused to assist LabMD's investigation by providing un-redacted versions of the Day Sheets. For three and one-half months, Commission staff did not inform LabMD that FTC had possession of the Day Sheets. However, Commission staff knew or should have known LabMD had an obligation under HIPAA to give notice of the unauthorized disclosure of PHI or PII. (Daugherty, Tr. 1027-1028) (Q. **"**What is it that you contend that the Federal Trade Commission didn't tell you?" A. "They didn't tell us they had the day sheets for three and a half months, even though we're subject to HIPAA, which requires us to notify in 60 days. . . . On the one hand we're supposed to protect patients and we're supposed to follow the law, and yet the federal government is withholding information from us, so it seems to me they're more eager to lambaste us and entrap us than keep patients safe. So we were outraged, scared, felt entrapped, and employees were starting to really break under pressure when that went down.").

Despite FTC's obstruction, LabMD timely notified everyone who could potentially have been affected and provided ample information to make people "aware of potential avenues" to mitigate the risk. *See Orkin Exterminating Co*, 849 F.2d at 1365. The notice included not only when, where, and what information may have been at risk, but also detailed instructions for

ordering a free credit report, an offer of free credit monitoring, and a hotline to call with questions.

4. Reliance.

Complaint Counsel has failed to prove LabMD unreasonably relied on its information technology specialists.

5. Unreasonable data security.

Complaint Counsel bears the burden of proving LabMD's data security was unreasonable. MTD Order at 18-19. However, as Fisk testified, the evidence is LabMD's data security was reasonable at all relevant times.

First, the origin of Complaint Counsel's entire case is Tiversa's LimeWire-enabled theft of the 1718 File on February 25, 2008. FTC had not warned the medical industry (or any other business sector) in any appropriate fashion about the risk of inadvertent file sharing through LimeWire as of February, 25, 2008. In fact, as FTC's partner Boback told Congress on May 5, 2009 (more than a year after the theft):

> [M]ost consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

Hearing on H.R. 2221, the "Data Accountability and Trust Act," and H.R. 1319, the "Informed P2P User Act," Before the Subcommittee on Commerce, Trade and Consumer Protection, 111th Cong. (May 5, 2009)(statement of Robert Boback, Chief Executive Officer, Tiversa at 4) *available at* http://democrats.energycommerce.house.gov/?q=hearing/hearing-on-hr-2221-the-data-accountability-and-trust-act-and-hr-1319-the-informed-p2p-user-a.

FTC, however, had been *partnering* for years with LimeWire and other P2P software providers. *See* FTC, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues,

at 26 (Jun. 2005); *see also* Letter from Deborah Majoras, Chairman of the FTC, to Rep. Henry Waxman, Chairman of OGR, at 2, Nov. 13, 2007, available at http://oversight-archive.waxman.house.gov/documents/20071128141924.pdf (last visited Oct. 6, 2014).[18]

In or about February, 2010, almost two years after Tiversa took the 1718 File in violation of state and federal law, and after FTC began its inquisition of LabMD, FTC first advised businesses that "[w]hen P2P file sharing software is not configured properly, files not intended for sharing may be accessible to anyone on the P2P network." *See* FTC, *Peer-to-Peer File Sharing, supra,*

The evidence is LabMD had policies in place at all relevant times prohibiting downloading of LimeWire. The policies were memorialized in documents including LabMD's Employee Handbook which required employees to comply with HIPAA under penalty of termination, prohibited employees from using LabMD computers for personal use, prohibited employees from downloading software without a valid business reason. LabMD monitored and enforced these policies by means including: daily IT walk-arounds, IT checks of employee computers, purchasing custom-designed Websense software, designating a compliance officer who provided trainings and advice, and preventing the computers of all but a few high-level employees from being able to download software.

As soon as LabMD was on notice that an employee may have violated its policies LabMD immediately took all reasonable steps to address the situation, including removing

[18]Discovery in this case has revealed FTC was working closely with Boback prior to the 2009 testimony. This raises interesting questions. Either Boback was correct, meaning FTC's failure to warn about P2P until January, 2010, was a monumental case of regulatory blindness, or FTC was correct and Boback was using Congress to create fear and sell product. If Boback was correct, and P2P was an insidious threat generally impervious to usual countermeasures, why did FTC not admit its error and change its ways? Or, if FTC was correct, and P2P was qualitatively no more of a threat than other internet-based applications, why was it enabling a charletan?

LimeWire from Woodson's computer, sending the computer to a forensic expert for examination, firing Woodson, and devoting weeks of employee time to monitoring P2P networks to ensure the 1718 File had not been exposed. Furthermore, LabMD purchased hundreds-of-thousands of dollars of additional IT software and hardware above and beyond other small laboratories and continually updated its Employee Handbook during the relevant time period in this case to reflect reasonable and adequate data security policies under HIPAA/HITECH for the medical industry.

LabMD's Day Sheets were stored only in hard copy form—in fact, they could not be stored electronically. Such documents could only have been physically removed from the facility and Dr. Hill opined LabMD's physical data security was adequate.

Complaint Counsel must prove by a preponderance of the evidence that there was an actual data breach *and*, if one occurred, that consumers suffer substantial injury *and* that LabMD's data security practices are "unreasonable." *See* MTD Order at 18-19; *Reilly*, 664 F.3d at 44-46; *HSBC Bank*, 691 F.3d at 1169. The Commission states "unreasonableness" is a "factual question that can be addressed only on the basis of evidence" but provides no additional guidance. MTD Order at 19.

Medical data security "reasonableness" under Section 5 as a matter of law is a matter of first impression. Section 5(n) does not define "unreasonable" data security acts or practices, or even use the term. Therefore, there is no statutory basis for a "reasonableness" determination. *See Steadman v. SEC*, 450 U.S. 91, 98 (1981). However, the MTD Order, though erroneous, is law of the case.

As a matter of law, FTC does not have the power to declare – for the first time through adjudication – conduct that is permitted by and compliant with HHS's preexisting regulatory

scheme, promulgated under HIPAA/HITECH in accordance with an act of Congress, unfair and unlawful under Section 5(n). *See Fabi Const. Co,*. 508 F.3d at 1088; *ABA v. Federal Trade Commission,* 430 F.3d 457, 469-72 (D.C. Cir. 2005); *Satellite Broadcasting v. FCC,* 824 F.2d at 3; *Gates & Fox v. OSHRC,* 790 F.2d 154,156-57 (D.C. Cir. 1986); *see generally* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566, 5,644 (Jan. 25, 2013)(encouraging covered entities to use encryption safe-harbor); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,543 (Dec. 28, 2000)(discussing safe-harbor).

As a matter of law, FTC should have published in the Federal Register applicable guides or policy statements prior to commencing regulation, as it has often done. *See* 16 C.F.R. § 14.9 (titled "Requirements concerning clear and conspicuous disclosures in foreign language advertising and sales materials," establishing same and warning "Any respondent who fails to comply with [the specified] requirement may be the subject of a civil penalty or other law enforcement proceeding for violating the terms of a Commission cease-and-desist order or rule"); 16 C.F.R. § 453.1 (funeral rule definitions); 15 U.S.C. 57a (stating Commission authority).

FTC may proceed by adjudication only in cases where it is enforcing discrete violations of existing laws and where the effective scope of the impact of the case will be relatively small and by § 57a procedures if it seeks to change the law and establish rules of widespread application. *Ford Motor,* 673 F.2d at 1010-11. Adjudication deals with what the law was; rulemaking deals with what the law will be. *Bowen,* 488 U.S. at 221. The function of filling in

the interstices of the FTC Act should be performed, as much as possible, "*through this quasi-legislative promulgation of rules to be applied in the future*." *See id.* (emphasis in original). Therefore, the Commission's adjudication is arbitrary and capricious. *Ford Motor,* 673 F.2d at 1010-11 (citation omitted). Complaint Counsel's failure to prove by a preponderance of the evidence that LabMD's data security currently violates, or is likely to violate in the future HIPAA/HITECH regulatory requirements, means that it has not proven unreasonableness as a matter of law.

A data security hearing under Section 5 is governed solely by the ordinary meaning of Section 5(a) and Section 5(n). *Steadman,* 450 U.S. at 98.

Complaint Counsel's position is that "[t]he enforcement of OSHA's General Duty Clause in Department of Labor administrative courts may provide the best analogy to a data security administrative hearing under Section 5 of the FTC Act. *See, e.g.*, *Fabi Constr. Co.,* 508 F.3d at 1088 (considering a number of factors to determine whether defendant met its 'general duty,' including whether defendant followed third-party technical drawings, whether defendant complied with industry standards, and expert opinion)." Complaint Counsel's Response In Opposition to Respondent's Motion to Dismiss Complaint, *In the Matter of LabMD, Inc.*, FTC Dkt. 9357, at 19 fn. 12 (Nov. 22, 2013).

Reasonableness is not whatever requirement the Commission determines, *post facto,* to have applied as if it were drafting a regulation. Rather, reasonableness is an objective test which must be determined on the basis of evidence in the record and "industry standards" are concrete and discernible standards applicable to a given company in its particular line of business. *See Fabi Constr. Co.*, 508 F.3d at 1084 (industry standards for a building construction company applied); *Ensign-Bickford Co.,* 717 F.2d at 1422 (industry standards for the pyrotechnic industry

applied); *S&H Riggers*, 659 F.2d at 1280-83 (reasonable-person standard divorced from relevant industry standards or regulations violates due process); *Diebold,* 585 F.2d at 1333 ("unless we embrace the untenable assumption that industry has been habitually disregarding a known legal requirement, we must conclude that the average employer has been unaware that the regulations required point of operation guarding").

LabMD is, as a matter of law, a HIPAA-covered entity and the relevant standards are those in effect for the medical industry and applicable to HIPAA-regulated entities. 45 C.F.R. § 160.103 "Covered entity"; *Fabi Constr. Co.*, 508 F.3d at 1084; *Ensign-Bickford Co.*, 717 F.2d at 1422; *S&H Riggers*, 659 F.2d at 1280-83 (reasonable-person standard divorced from relevant industry standards or regulations violates due process); *Diebold,* 585 F.2d at 1333. Industry standards and customs are not entirely determinative of reasonableness because there may be instances where a whole industry has been negligent. *See Bristol Steel & Iron Works, Inc. v. OSHRC*, 601 F.2d 717, 723 (4th Cir. 1979)("the appropriate inquiry is whether under the circumstances a reasonably prudent employer familiar with steel erection would have protected against the hazard of falling by the means specified in the citation"). However, such negligence on the part of a whole industry cannot be lightly presumed and must be proven. *Diebold*, 585 F.2d at 1333.

Applicable medical industry standards were and are readily available. *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. at 8344; 45 C.F.R. §§ 164.400-414 (breach notification rule); FTC, "Complying with the FTC's Health Breach Notification Rule," https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule (last visited August 9, 2015); HHS, "HIPAA Security Series: Security 101 for Covered Entities,"

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (last accessed Aug. 9, 2015). LabMD and all other covered entities in the medical industry must follow HIPAA, HITECH, and HHS PHI data security regulations. *See e.g.* Applicability of Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164.302 (2014) ("A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity"); 45 C.F.R. § 160.103 (2014)(definition of a "covered entity"). LabMD has not violated HIPAA/HITECH. *See* Complaint Counsel's Amended Response To LabMD, Inc.'s First Set Of Requests For Admission, *In the Matter of LabMD*, Dkt. No. 9357, Responses No. 7 and No. 8, at pp. 8-9, appended to Complaint Counsel's Motion to Amend Complaint Counsel's Response to Respondent's First Set of Requests for Admission (April 1, 2014); *see also,* Complaint, *In the Matter of LabMD,* Dkt. No. 9357 (Aug. 28, 2013).

It is arbitrary, capricious, contrary to law, and a violation of due process for Complaint Counsel to allege and/or the Commission to determine unreasonableness without specific reference to HIPAA/HITECH standards and regulations. *See Fabi Constr. Co.*, 508 F.3d at 1084; *Ensign-Bickford Co.*, 717 F.2d at 1422; *S&H Riggers*, 659 F.2d at 1280-83. In any event, Complaint Counsel has failed to prove by a preponderance of the evidence that the entire medical industry was negligent or that HIPAA/HITECH regulations and standards were or are inadequate or that LabMD's conduct was "unreasonable." *See Diebold,* 585 F.2d at 1336. [19]

[19] As a matter of law, if Respondent reasonably relied on experts to design and implement its information technology system, then its data security practices cannot be "unreasonable." *See R.P. Carbone Constr. Co. v. OSHRC,* 166 F.3d 815, 819-20 (6th Cir. 1998)(reasonable reliance on subcontractors who were experts relieves contractor from liability)(citation omitted).

D. Complaint Counsel's Requested Relief Fails.

Complaint Counsel has not proven it is entitled to the requested relief.

First, Section 5(b) did not specifically authorize the Commission to issue a Notice Order with the Complaint. Consequently, the Notice Order in this case is either a judicially reviewable final order, or it demonstrates prejudgment and violates due process, or it is an ultra vires act in violation of the APA.

Second, the Notice Order is not equitable but punitive in nature and the Commission is not authorized to issue it. *Heater v. FTC*, 503 F.2d 321, 322-327 (9th Cir. 1974) (Overturning an FTC order for restitution as inconsistent with the purpose of the FTC Act, which does not authorize punitive or retroactive punishment); MTD Order at 18 ("fact-finders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages.").

The Commission wrongly argued that because it is not pursuing criminal or civil penalties for past conduct it need not provide fair notice. However, even if this argument were not incorrect, *see, e.g.*, *United States v. Chrysler Corp.*, 158 F.3d 1350, 1354-55 (D.C. Cir. 1998); *In re Bogese*, 303 F.3d 1362, 1368 (Fed. Cir. 2002); *PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000), the evidence does not support the claimed relief.

The MTD Order was issued a mere 16 days after LabMD announced that due to FTC's actions the company was shutting down operations and began to transition its PHI out active use and to secure storage.

Complaint Counsel's own expert, Hill, has admitted that LabMD's physical security is adequate. (Hill, Tr. 293).

Given that LabMD is no longer using PHI in its daily operations, but instead is storing it securely, there is no basis in law to require LabMD to comply with requirements such as establishing a "comprehensive information security program," hiring outside professionals to conduct biannual audits, and hiring additional personnel to monitor the security of data that is not being actively used and is being kept on computers that are stored with the power off. In fact, there *can be no equitable purpose* for requiring LabMD to follow senseless rules that have no actual impact on the security of its PHI data. *Accord Borg-Warner, supra.*

Complaint Counsel has failed to prove by a preponderance of the evidence that LabMD's past course of conduct is a basis for believing it will violate Section 5(n) in the future. For example, the evidence is LabMD had robust PHI protection, including both technical and human factors measures. These measures satisfied HHS and LabMD's customers, and were so effective that FTC has been unable to identify even a single patient who suffered harm of any sort due to LabMD's data security acts or practices at any time.

Also, there is no equitable purpose to requiring LabMD to notify consumers because the evidence is LabMD already notified all of the consumers it had a duty to notify. *See* HIPAA Breach Notification Rule, 45 CFR § 164.400 (2014) ("Applicability."); (Daugherty, Tr. 1027-1028) (Q. **"**What is it that you contend that the Federal Trade Commission didn't tell you?" A. "They didn't tell us they had the day sheets for three and a half months, even though we're subject to HIPAA, which requires us to notify in 60 days. . . . On the one hand we're supposed to protect patients and we're supposed to follow the law, and yet the federal government is withholding information from us, so it seems to me they're more eager to lambaste us and entrap us than keep patients safe. So we were outraged, scared, felt entrapped, and employees were starting to really break under pressure when that went down.").

Third, the Notice Order requires LabMD to hire outside contractors to conduct biannual assessments, send letters to all persons on the 1718 File (notwithstanding there is no evidence of breach or injury) and establish a hotline and website, implement onerous document retention requirements, and meet agency reporting requirements for twenty years. *See* Complaint, *In the Matter of LabMD*, Dkt. No. 9357, at 12, Aug. 28, 2013. However, the Commission's demand for this "fencing-in" relief is unsupportable.

Any relief the Commission demands must be reasonably related to a violation Section 5. *See In re Daniel Chapter One*, 2009 FTC LEXIS 157, at *280-281 (citations omitted). Whether fencing-in relief bears a "reasonable relationship" to the conduct found to be unlawful depends on: "(1) the deliberateness and seriousness of the violation; (2) the degree of transferability of the violation to other products; and, (3) any history of prior violations." *Id*. Such relief must be "reasonably calculated to prevent future violations of the sort found to have been committed," *see ITT Continental Baking Co. v. FTC*, 532 F.2d 207, 221-22 (2d Cir. 1976), and is judged based on the "the likelihood of the petitioner committing the sort of unfair practices" that have been prohibited. *See Borg-Warner, supra; Litton Industries, Inc. v. FTC*, 676 F.2d 364, 371 (9th Cir. 1981).

Complaint Counsel has failed to prove by a preponderance of the evidence that fencing-in relief is proper. *See In re Daniel Chapter One*, 2009 FTC LEXIS 157, at *280-281. It has failed to allege or prove LabMD knowingly violated Section 5 or that its violations were "serious."

Complaint Counsel does not dispute that LabMD's data security between January, 2005, and July, 2010, complied with HIPAA and the Commission has not alleged that a HIPAA-compliant data security program could be in "serious" violation of Section 5. *Compare In the Matter of Daniel Chapter One*, 2009 FTC LEXIS 157, at *281-282; *In the Matter of POM*

Wonderful LLC, 2012 FTC LEXIS 18, at *97-98 (FTC Jan. 11, 2012). Additionally, Complaint Counsel has failed to prove the requisite "degree of transferability of the violation to other products." *See In re Daniel Chapter One*, 2009 FTC LEXIS 157, at *280-281. Finally, it has not alleged or proven a "history of prior violations." *See id.* Consequently, fencing-in relief is both unnecessary and unlawfully punitive in this case. *See* (Daugherty, Tr. 939-978, 130-133); (CX0741 (Van Dyke, Rep. at 21)); (Van Dyke, Tr. 692-693); (RX523 (Van Dyke, Dep. at. 70-71)); *see also Riordan v. SEC*, 627 F.3d 1230, 1234 (D.C. Cir. 2010)("we have stated that a cease-and-desist order is 'purely remedial and preventative' and not a 'penalty' or 'forfeiture.'").

The Notice Order also includes a prohibited "obey-the-law" provision. It provides LabMD must:

> [N]o later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:
>
> > A. The designation of an employee or employees to coordinate and be accountable for the information security program;
> >
> > B. The identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

> C. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
>
> D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
>
> E. The evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

(Compl. at 7-8).

If FTC gave LabMD notice during the relevant time (2005-2010) that Section 5 required these things, as Complaint Counsel has argued it has, then the proposed order is an invalid "obey-the-law" provision. *SEC v. Goble*, 682 F.3d 934, 949 (11th Cir. 2012). If FTC did not give LabMD notice during the relevant time that Section 5 required these things, then, by definition, LabMD lacked constitutional fair notice. *Fabi Constr. Co.*, 508 F.3d at 1088.

Conclusion

The Commission lacked both the power and the evidence it needs to justify the damage it has done in this case to LabMD. The government's partnership with Tiversa, and its blind eye to Tiversa's obvious *crimes*, cannot be explained, glossed over or rationalized. 42 U.S.C. § 1320d-6 means what it says, but FTC seems to have been otherwise engaged.

By taking action against LabMD, FTC has exceeded its statutory bounds, violated the Constitution, and repeatedly acted arbitrarily and capriciously contrary to the Administrative

Procedure Act. Furthermore, Complaint Counsel has not proven by preponderant evidence that LabMD's data security acts or practices between January, 2005, and July, 2010, "cause" now or "are likely to cause" in the future substantial consumer injury. The Commission has yet to establish LabMD did anything contrary to the prevailing standards in the medical industry at any time between January, 2005, and July, 2010.

For all of the reasons set forth above, judgment for LabMD is proper.

/s/ Daniel Z. Epstein
Daniel Z. Epstein
Prashant K. Khetan
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW Suite 650
Washington, DC 20006
Phone: (202) 499-4232
Facsimile: (202) 330-5842
Email: daniel.epstein@causeofaction.org

Counsel for Respondent

/s/ *Reed D. Rubinstein*
Reed D. Rubinstein
William A. Sherman, II
Sunni R. Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW
Suite 610
Washington, DC 20004
Phone: (202) 372-9100
Facsimile: (202) 372-9141
Email: reed.rubinstein@dinsmore.com

Counsel for Respondent, LabMD, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on August 11, 2015, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

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

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

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

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

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

Dated: August 11, 2015 /s/ Patrick J. Massari

CERTIFICATE OF ELECTRONIC FILING

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

Dated: August 11, 2015 /s/ Patrick J. Massari

Notice of Electronic Service

I hereby certify that on August 11, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Post-Trial Brief (PUBLIC), with:

D. Michael Chappell
Chief Administrative Law Judge
600 Pennsylvania Ave., NW
Suite 110
Washington, DC, 20580

Donald Clark
600 Pennsylvania Ave., NW
Suite 172
Washington, DC, 20580

I hereby certify that on August 11, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Post-Trial Brief (PUBLIC), upon:

John Krebs
Attorney
Federal Trade Commission
jkrebs@ftc.gov
Complaint

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Jarad Brown
Attorney
Federal Trade Commission
jbrown4@ftc.gov
Complaint

Kent Huntington
Counsel
Cause of Action
cmccoyhunter@ftc.gov
Respondent

Sunni Harris
Esq.
Dinsmore & Shohl LLP
sunni.harris@dinsmore.com
Respondent

Daniel Epstein
Cause of Action
daniel.epstein@causeofaction.org
Respondent

Patrick Massari
Counsel
Cause of Action
patrick.massari@causeofaction.org
Respondent

Prashant Khetan
Senior Counsel
Cause of Action
prashant.khetan@causeofaction.org
Respondent

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

Laura Riposo VanDruff
Federal Trade Commission
lvandruff@ftc.gov
Complaint

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

Erica Marshall
Counsel
Cause of Action
erica.marshall@causeofaction.org
Respondent

Patrick Massari
Attorney