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

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

RESPONDENT LABMD, INC.'S CORRECTED[1] PROPOSED FINDINGS OF FACT

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

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

Dated: August 11, 2015

Counsel for Respondent

[1] This document was timely filed on August 10, 2015. It is being re-filed solely to correct errors in the redaction process, mostly due to making redactions using a computer tool that does not transmit when converted to pdf and filed electronically. Counsel for LabMD has been in constant discussion with Complaint Counsel as well as Crystal McCoy Hunter in the Office of the Secretary regarding these issues.

TABLE OF CONTENTS

RECORD REFERENCES

References to the record are made using the following citation forms and abbreviations:

JX# – Joint Exhibit

CX# – Complaint Counsel Exhibit

RX# – Respondent Exhibit

RXD# – Respondent Demonstrative Exhibit

(Name of Witness, Tr. xx – Trial Testimony

JX/CX/RX# (Name of Witness, Dep. at xx) – Deposition Testimony

JX/CX/RX# (Name of Witness, IHT at xx) – Investigational Hearing Testimony

Complaint ¶ x – Complaint Counsel's Complaint filed August 28, 2013

Answer ¶ x – Respondent LabMD, Inc.'s Answer to Complaint

{ bold } – *In Camera* Material

A. Background

1. The Federal Trade Commission ("FTC" or the "Commission") initiated an investigation of Respondent, LabMD, Inc. ("LabMD") in January 2010.

2. The Commission acted against LabMD based on information obtained from Tiversa, Inc. ("Tiversa"), through the "Privacy Institute" in 2009. (CX0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX0703 (Boback, Dep. at 141-142)).

3. The Privacy Institute was created to share information between the Commission and Tiversa. (CX 0703 (Boback, Dep. at 141-142); (RX 541 (Boback, Dep. at 37-38, 47-49)) (" … [on the] spreadsheet that the Privacy Institute received from Tiversa, which the Privacy Institute later provided to the FTC pursuant to [the] CID, ... [t]here were a list of [approximately 100] companies, names. There were, to the best of my recollection, a listing of how many social security numbers were exposed in a descending order. . . [and] Tiversa created the spreadsheet . . . [because] Tiversa provides security services on file sharing networks in which it is quite common to see large disclosures of social security numbers on these networks. And pursuant to the CID that [information request] went to the Privacy Institute, [and then] Tiversa searched Tiversa's data store for anything responsive of that CID, created the spreadsheet, [and] provided the spreadsheet to the Privacy Institute. And then, the Privacy Institute, pursuant to the CID, provided it to the FTC, to the best of my knowledge."), 54-55 ("I think we already were clear that the Privacy Institute did not have operations … The Privacy Institute didn't do anything.").

4. The Commission and Tiversa collaborated beginning in 2007. (Wallace, Tr. 1346-1349) (Q. "After the testimony at the congressional hearing for which you provided some documentation, did there begin to be communications between Tiversa and the FTC?" A. "Yes."

Q. "How soon after the congressional hearing did these communications begin?" A. "I couldn't say for sure, but I would venture to speculate maybe around two months after." Q. "And were you present during these communications?" A. "Yes." Q. "And how often were these communications occurring once they began?" A. "There were different things happening, so sometimes there would be communication that was quite frequent, other times, you know, maybe weekly."); (RX644[2] (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? 56 (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA), *available at* http://www.scribd.com/doc/265820770/2015-01-02-Staff-Report-for-Rep-Issa-Re-Tiversa#scribd (last visited Aug. 9, 2015) ("***In October 2007, Boback participated in a conference call with FTC officials*" and in "*December 2007, Boback provided documents to the FTC***." (emphasis added and citations omitted).

5. As a result of the Commission's collaboration with Tiversa, the Commission issued a February 22, 2010 press release titled "Widespread Data Breaches Uncovered by FTC Probe." (Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Fed. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015).

6. In this press release, the Commission stated: "we found health-related information,

[2] Respondent notes this Court's ruling on RX 644: "RX 644 is hereby admitted subject to the following limitations and qualifications as to its evidentiary use: (1) official notice is taken of the fact that the OGR investigated the activities of non-party witness Tiversa, Inc. ("Tiversa") and of the conclusions of the OGR staff as to the truthfulness and completeness of the information provided to the FTC by Tiversa and its president, Robert Boback; (2) statements purportedly made by Mr. Boback to the OGR, to the extent referred to in RX 644, will not be considered for the truth of the matters asserted therein; and (3) documents provided to OGR, to the extent referred to in RX 644 and not previously admitted into evidence in this case, will not be considered for the truth of the matters asserted therein." Order on Respondent's Motion to Admit Exhibits at 3 (July 15, 2015).

financial records, and drivers' license and social security numbers--the kind of information that could lead to identity theft …" and that it "notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, ha[d] been shared from the organizations' computer networks." (Press Release, Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015).

7. The information "found" by the Commission was actually given to it by Tiversa. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX 0703 (Boback, Dep. at 141-142)).

8. This information included an insurance aging file (the "1718 File") from LabMD containing personal health information ("PHI"). (Wallace, Tr. 141); (Shields, Tr. 876-881).

9. At all times relevant, the Commission knew or should have known that 42 U.S.C. § 1320d-6 provides that: "[a] person who knowingly and in violation of this part … (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization."

10. At all times relevant, the Commission knew or should have known that Tiversa was not authorized by LabMD or by any of the patients listed on the 1718 File to obtain or disclose the identifiable health information contained therein.. (CX 0679 (Verified Complaint for Declaratory

and Injunctive Relief (N.D. Ga.), at at 5-6 ¶ 16)) ("At all times relevant, LabMD's Protected Health Information ('PHI'), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), 42 U.S.C. §§ 300jj *et seq*., 17901 *et seq*.").

10. January 2005 through July 2010 is the relevant time period during which the Commission claims LabMD's data security was inadequate, unreasonable and unlawful ("Relevant Time"), (Hill, Tr. 221-222), and that these inadequacies "caused" or are "likely to cause" substantial consumer injury which cannot reasonably be avoided. (Complaint, at 5 ¶ 22 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

11. The Commission has never alleged that LabMD's post-July 2010 data security was inadequate. (Complaint, at 4-5 ¶¶ 17-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357); (CX 0740 (Hill, Rep. at 3-4 ¶¶ 4, 48)) ("This conclusion covers the time period from January 2005 through July 2010 (Relevant Time Period); as I explain in Paragraph 48, below, from my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.") ("As I noted in Paragraph 4, above, my overall conclusion and the specific opinions that support that conclusion cover the Relevant Time Period, which is January 2005 through July 2010. From my review of the record, there are not sufficiently diverse types of information available after the Relevant Time Period for me to offer opinions about that period.").

B. LabMD

12. LabMD is a small, medical services company providing uro-pathology cancer

detection services to physician customers. (Daugherty, Tr. 952).

13. LabMD, was incorporated in 1996 by Michael J. Daugherty ("Daugherty"), its President and CEO. (Daugherty, Tr. 939).

14. LabMD began in 1996 primarily as a men's health clinic. (Daugherty, Tr. 939-940).

15. Prior to founding LabMD, Mr. Daugherty worked for 13 years in the hospital and healthcare field as part of Mentor Corporation as a Surgical Sales Technical Representative working in the Urology and Plastic Surgery marketplace. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld, at 2)).

16. While working as a Surgical Sales Representative, Mr. Daugherty was "trained at US Surgical in Connecticut over a two–month period on aseptic technique, patient privacy, confidentiality, surgical technique" and "scrubbed in" with the surgeons. (Daugherty, Tr. 938).

17. LabMD changed its business model in the 1990s to meet a demand in the market for physicians who wanted their tissue samples analyzed by a specialist, which was made possible by mobile ultrasound machines. (Daugherty, Tr. 941-943).

18. Managed care exploded in the 1990s resulting in the requirement that physicians' offices direct tissue samples to a particular laboratory covered by their patients' health insurance. (Daugherty, Tr. 944-945).

19. LabMD's niche in the area of uro–pathology was creating technology whereby physicians' patient databases were coded, so tissue sample requests could be sent to LabMD without physicians' staff needing to spend time coding the samples by hand. (Daugherty, Tr. 959-960) (Q. "So what process did you put in place?" A. ". . . what we did was we would go into a[n] account, a physician's office. We would get their entire insurance database, and we would

give it a primary additional code. . . . [W]e had the database populated with all the patients that were in the physician's office, so that saved all this time. . . . This is proactivity to increase patient result speed because people want to know if they do or don't have cancer as soon as possible, reduce any pitfalls of error. It's just a win-win everywhere.").

20. The system was set up to limit access of physicians to their patients' information only. (CX 0719 (Hyer, Dep. at 142)).

21. LabMD created a process to streamline the interaction between physicians' offices requesting lab work and LabMD's delivery of the diagnosis of the lab work requested. (Daugherty, Tr. 955-964).

22. LabMD's process resulted in faster lab results turnaround time and fewer diagnosis code errors. (Daugherty, Tr. 961-962).

23. LabMD provided a valuable and necessary service in the uro-pathology marketspace. (Daugherty, Tr. 962) (A. "And in our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices. . . . [T]he amount of errors just fell through the floor. . . . [W]e even knew ahead of time what was coming so that we could be prepared.").

24. The tissue slides were received into the LabMD facility where the histologist puts each sample into its proper cartridge. (Daugherty, Tr. 968; RXD 04).

25. LabMD only analyzed one type of tissue, which allowed for 30-minute processing time as opposed to 12 hours. (Daugherty, Tr. 968-969).

26. After the tissue was completely dehydrated, it was placed in an embedding center

where hot wax is poured over the sample to hold it firmly in place for cutting. (Daugherty, Tr. 969; RXD 06).

27. The histotech then utilized the microtome "to cut the tissue one cell thick" for testing and analysis. (Daugherty, Tr. 969; RXD 07).

28. The tissue was then placed "in a wax ribbon that is now one cell thick along the ribbon, and … put in a water bath to rehydrate …" (Daugherty, Tr. 970; RXD 08).

29. RXD 10 is a tissue slide with identifying numbers showing case number and exact location within the gland. (Daugherty, Tr. 970-971; RXD 10) (". . . the last two digits are going to show the exact location within the gland. The top number in the center is the case number that is assigned electronically by the software back in the urologist's office when the nurse places the order. So at this point all these slides have had the proper, very legible information put on each one, so the correct tissue ribbon is put on each slide and they're ready to go to be stained.").

30. The tissue sample was then placed in the Sakura stainer, which is part of the diagnosis protocol proper. (Daugherty, Tr. 971; RDX 11) (A. ". . . Different types of cancer cells need different types of stains. And not only is the type of stain relevant, but the amount of time immersed in the stain and the time immersed and the order of immersion is relevant to making the cancer cells pop out so it's easy to diagnose for the physician. . . . this is a phenomenal machine because it is -- it makes sure that every single tissue slide location is stained properly, recorded. It's—it's fantastic.").

31. The tissue slides were then taken out of the stainer and "started to be prepped for the physician's diagnosis to start." (Daugherty, Tr. 972; RXD 12).

32. The tissue sample was then placed into a final folder so the on-site physician at

LabMD could begin “reading each slide location” and making a diagnosis. (Daugherty, Tr. 973; RXD 13; RXD 14).

33. LabMD retained these samples and made them available to physicians for years. (Daugherty, Tr. 972).

34. LabMD’s coding and numbering system benefitted both the patients and physicians it served. (Daugherty, Tr. at 972) (A. “. . . the center number is the accession number. The LM is the location of the gland. The number below L2 is the level, because we'll keep several levels of the tissue because we need to keep this for years to come in case a second opinion is wanted, there’s litigation, there’s clinical questions years down the road, so we take several levels of the tissue and hold them.”).

C. <u>The Origins of FTC’s Investigation of LabMD</u>

35. On July 24, 2007, the CEO of Tiversa, Robert Boback (“Boback”) testified before a congressional committee concerning the serious data security risks posed by P2P file sharing programs. (Wallace, Tr. 1341-1342).

36. According to CEO Robert Boback, Tiversa was incorporated in 2004. (CX 0703 (Boback, Dep. at 11)).

37. Tiversa provides information and security services which essentially consist of P2P breach detection and remediation. (CX 0703 (Boback Dep. at 10-12); RX 541 (Boback Dep. at 19-21)).

38. Tiversa has nearly 120 patents or patents pending for software providing unique searches of internet file sharing networks. (CX 0703 (Boback Dep. at 10-12); RX 541 (Boback Dep. at 19-21)).

39. Tiversa has received direct payment from the federal government for providing services to the FBI and the Department of Transportation. (CX 541 (Boback, Dep. at 64, 38-41); (Complaint Counsel's Opposition to Respondent's Motion for Sanctions at 6 n.6 (Aug. 25, 2014)) ("Tiversa received no government funds for the work it performed with researchers at Dartmouth College, including work related to the Data Hemorrhages article, in which the 1718 File is excerpted (CX0382). *See, e.g.*, CX0703 at 134; RX541 at 56.").

40. However, ***in response to an unanticipated question during Complaint Counsel's May 20, 2014 opening statement, Complaint Counsel mistakenly stated that Tiversa had received no federal funding.*** (*Compare* Compl. Counsel's Opposition to Respondent's Motion for Sanctions at 6 (Aug. 25, 2014) *with* RX 541 (Boback, Dep. at 14)).

41. During the November 21, 2013 deposition of Tiversa's Rule 3.33 designee, Complaint Counsel did not develop any facts regarding Tiversa's contracts with government agencies. (CX 0703 (Boback, Dep. at 1-168)).

42. At a Congressional hearing before the House Oversight and Government Reform Committee on July 24, 2007, the Commission testified that it viewed P2P file sharing as a "neutral technology." (CX703 (Boback, Dep. at 139-140); (*Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform,* 110th Cong., 1st Sess. 1 10, 40-84 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last visited Aug. 9, 2015)).

43. The Commission's position at the July 24, 2007 Congressional hearing was:

- "P2P file-sharing ... is a 'neutral' technology" and there was "little empirical evidence" regarding relative P2P risks "compared to the risks from other Internet-related activities."

- "FTC will continue to assess [P2P] risks..., educate consumers, monitor and encourage [P2P] industry self-regulation, and investigate and institute law enforcement actions [against P2P companies] when appropriate."
- FTC's "twenty-first century law enforcement tools" included "Consumer Sentinel, a secure, online fraud and identity theft complaint database" containing "over 3.9 million fraud and identity theft complaints [that is] accessible to more than 1,650 law enforcement agencies, which use the database to share information, coordinate investigations, and pursue case leads," as well as "Internet Lab, which provides FTC lawyers and investigators with high-tech tools to ... capture web sites that come and go quickly ...[and] FTC staff with the necessary equipment to preserve evidence for presentation in court."

(Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 3, 8 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)) (Statement of Mary Engle, Assoc. Dir. for Advertising Practices. Fed. Trade Comm'n), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf (last accessed Aug. 9, 2015).

44. FTC had not warned businesses of the risk of inadvertent file sharing through LimeWire in February, 2008, when Tiversa hacked LabMD for Tiversa's commercial interest. (Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 10, 40-84 (July 24, 2007), *available at*

http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)) ("The [2005 FTC Report] emphasized that many of the risks posed by P2P file sharing also exist when consumers engage in other Internet-related activities, such as surfing Web sites, using search engines, or e-mail.…"); (FTC Staff Report, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, at 20 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015)) ("***Although it has required warnings with respect to inherently dangerous products, the Commission concluded that it was not aware of any basis under the FTC Act for requiring warnings for P2P file sharing and other neutral consumer technologies***.") (emphasis added).

45. The FTC's considered position for the period of 2005–2008 was that using P2P networks like LimeWire or FrostWire was not in and of itself an unreasonable practice from the viewpoint of data privacy and security. (Prepared Statement of Mary Engle, Fed. Trade Comm'n, Assoc. Dir. for Advertising Practices, Before the U.S. House of Rep. Committee on Oversight and Government, Washington, D.C., at 1–12 (July 24, 2007), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-peer-peer-file-sharing-technology-issues/p034517p2pshare.pdf (last accessed Aug. 9, 2015)).

46. FTC worked with LimeWire and other P2P software providers to encourage industry self-regulation. (Fed. Trade Comm'n, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, Staff Report, at 26 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015))

("FTC staff encourages the P2P file-sharing industry to continue its efforts to decrease these risks through technological innovation and development, industry self-regulation (including risk disclosures), and consumer education.").

47. The Commission did not warn businesses about the dangers of P2P networks until after it commenced action against LabMD in January 2010. (Fed. Trade Comm'n, Peer-to-Peer File Sharing: A Guide for Business, (January 2010), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business (last accessed Aug. 9, 2015)).

48. In July, 2007, Richard E. Wallace ("Wallace") was hired by Boback and Tiversa as a forensic analyst. (Wallace, Tr. at 1337, 1339-1340).

49. Wallace prepared the materials used by Boback and Tiversa at a July 24, 2007 hearing before the United States House of Representatives Committee on Oversight and Government Reform ("OGR"), Chairman Henry Waxman presiding. (Wallace, Tr. 1341-1342).

50. Boback and Tiversa lied to Congress when Boback stated to OGR on July 24, 2007 that Tiversa's systems had obtained all files and information downloaded from P2P networks. (Wallace, Tr. 1432-1433).

49. Wallace handled "special projects" for Boback. (CX 0872 (Gormley. Dep. at 82-83)).

50. Wallace scoured P2P networks and downloaded information from the Gnutella protocol networks. (Wallace, Tr. 1340).

52. Boback instructed Wallace to "use any and all means available to find information … [e]verything from health insurance information to [] PII, Social Security numbers, basically anything that should not be out [] on these networks." (Wallace, Tr. at 1341-1342).

51. "Tiversa's platform was a series of algorithms that allowed the entire peer-to-peer network to be captured not going any deeper into any computer system but just has more breadth." (Wallace, Tr. 1340).

52. Tiversa claimed that its technology enabled it view the entire P2P network and thus provide real-time, actionable information regarding sensitive file disclosures. (Inadvertent File Sharing Over Peer-to-Peer Networks: Hearing Before the House Comm. on Oversight Gov't Reform, 110th Cong., 20 (July 24, 2007) (written statement of Robert Boback, Chief Exec. Officer, Tiversa, Inc.), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015)).

53. Tiversa's "data store" was a depository of long servers containing data that is pulled in from different networks or peer-to-peer networks. (Wallace, Tr. 1371) (JUDGE CHAPPELL: "'Data store,' what does that mean?" THE WITNESS: "It is a depository of ICE long servers that as data is pulled in from different networks or peer-to-peer networks, it's stored in the data store." JUDGE CHAPPELL: "Was it something on your computer, your server at Tiversa?" THE WITNESS: "Yes. It would be accessible from a workstation at Tiversa. There are several workstations." JUDGE CHAPPELL: "And what was in the data store?" THE WITNESS: "That would be hard copies of files that were downloaded from the Gnutella network." JUDGE CHAPPELL: "This would not be where these IP addresses would be located." THE WITNESS: "Yes." JUDGE CHAPPELL: "It would be or would not be?" THE WITNESS: "It would be." JUDGE CHAPPELL: "So that was also there, where a file could be located, as well as the actual file?" THE WITNESS: "Yes.").

54. Wallace would search and download files from the P2P networks, often without using Tiversa's search platform, which were then injected or "supplemented" into Tiversa's data

store. (Wallace, Tr. 1342-1343) (JUDGE CHAPPELL: "… I've heard you talk about viewing, searching and downloading. In the context of your job at Tiversa, tell me what each term means, 'downloading,' 'viewing' and 'searching.' Did you do all of these or do they mean the same thing? Tell me what they meant in the context of your work." THE WITNESS: "There were multiple positions -- or multiple activities under my position. One of them would have been, you know, using a standard, off-the-shelf peer-to-peer client, such as LimeWire or BearShare or Kazaa or Morpheus, any of those that are, you know, affiliated with the Gnutella network. I would be able to use those clients to supplement other information that Tiversa's system possibly hadn't downloaded. So it would be just another tool to supplement the information that Tiversa would have in the data store.").

55. Wallace decided what to download without a set of written parameters. (Wallace, Tr. 7-16) (JUDGE CHAPPELL: "Who made the decision of what to download?" THE WITNESS: "That would be the person sitting at the keyboard, so me." JUDGE CHAPPELL: "Did you have a set of written parameters like if you find this, you download it, or how did that work?" THE WITNESS: "No. Because it would be very difficult to know what's inside of a file prior to downloading it.").

56. Wallace worked hand-in-hand with Boback, who decided how to best "monetize th[e] information" by contacting potential targeted entities as well as existing clients about the fraudulent "spread," or proliferation, of the P2P files on the Internet. (Wallace, Tr. 1344) (JUDGE CHAPPELL: "And once you downloaded a file, what did you do with it? Did you decide that, okay, this is worth something and then you tell Mr. Boback?" THE WITNESS: "Yes." JUDGE CHAPPELL: "How did that process work?" THE WITNESS: "***Basically, I worked very closely at the time with Bob Boback. If it was something of -- significant in***

nature, then I would definitely go to Bob and say this is what we have, you know, and he would make the decision at that point how to best monetize that information, whether it be giving it to a salesperson or him calling the company directly.") (emphasis added); (Wallace, Tr. at 1361) (JUDGE CHAPPELL: "***And you used the word I think 'monetize'?***" [WALLACE]: "***Yes.***" JUDGE CHAPPELL: "***Something that could be monetized?*** [WALLACE]: ***We -- early on, we were having problems at Tiversa, we were having problems selling a monitoring contract, so we started contacting individual companies when information came out, and you would be able to charge them a lesser amount than a yearlong contract, just basically a one-off to take care of that problem right then.***") (emphasis added).

57. When Wallace downloaded or "pulled down" files from P2P networks, he recorded the type of file and the file's IP address at the time of the download. (Wallace 1344-1345) (BY MR. SHERMAN: Q. "So, Mr. Wallace, when you were viewing files, is it correct to say that when you were viewing files on the network, you were not actually viewing the content of those files?" A. "***You would start out by viewing the file title, the type of file that it is, and you would record the IP and port.*** …" Q. "…***You used the term 'pull down.' Does that mean that you would download those files?***" A. "***Yes.***") (emphasis added).

49. On or about February 25, 2008, Rick Wallace, on behalf of Tiversa, downloaded a LabMD insurance aging file that was 1,718 pages in length from a LabMD workstation located in Atlanta, Georgia, at IP address 64.190.82.42. (Wallace, Tr. 1441).

50. Wallace was a uniquely skilled computer analyst, especially adept at using P2P networks, and he was engaged in a focused search to uncover commercially valuable data at the expense of unsuspecting victims. (Wallace, Tr. 1339-1391).

51. Wallace was a law enforcement asset. (Wallace, Tr. 1369, 1445).

52. Wallace was hired by Boback to help generate business. (Wallace, Tr. 1344, 1360-1361, 1364).

53. Wallace acted as an instrument of and abettor for Boback and Tiversa in defrauding LabMD and Tiversa's clients. (Wallace, Tr. 1366-1367).

54. Tiversa's business model was to take files, manufacture "spread" using false IP addresses so that they appeared to be available on the Internet, and then sell "remediation" services to the victimized companies. (Wallace, Tr. 1366-1367).

55. Boback and Tiversa directed Wallace to intentionally create the illusion that companies' PII and/or PHI was widely available on P2P networks. (Wallace, Tr. 1367-1368) (Q. ***"Can you explain to us how you would make it appear as though the data had proliferated?" A. "Sure. So as we talked about earlier, if you use a stand-alone client like a LimeWire or Kazaa or BearShare or whatever you have to supplement the data store with information, there is a folder that I would direct – or that I would put files in that would show up in the data store, you know, with Coveo or whatever application you're using to have a front end. It would show up just like it was downloaded from that IP***. …") (emphasis added); (JUDGE CHAPPELL: "***Let me get this straight. … You actually did it. You actually made it available around the Internet in peer-to-peer*** — [WALLACE]: "***No. No. We would only make it appear to have been downloaded from a known bad actor. So if you have an identity thief in Arizona, say, for example, we already know law enforcement has already dealt with that individual. We know that the IP is dead. We know that the computer is long gone. Therefore, it's easy to burn that IP address because who's going to second-guess it." JUDGE CHAPPELL: "So to boil this down, you would make the data breach appear to be much worse than it actually had been." [WALLACE]: That's correct.***") (emphasis added).

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

57. The list of IP addresses on CX0019 was created by Wallace at Boback's express direction containing known criminals' IP addresses on P2P networks obtained by Wallace, as well as the date and time the file was "modified" and appended with LabMD's stolen insurance aging file, and then injected into Tiversa's data store. (Wallace, Tr. 1374-1385).

58. Wallace and Boback met with FTC officials, including but not limited to Complaint Counsel Alain Sheer, with a view towards create a wholly false document which would make it appear that LabMD's insurance aging file had spread on P2P networks, when in fact that was never the case. (Wallace, Tr. 1386-1388) (Q. ***"Who traveled to D.C. [to meet with***

Alain Sheer and FTC] from Tiversa?" A. "***Bob Boback was driving. I was in the car, Anju Chopra and Keith Tagliaferri.***" Q. "***Following the meeting, did the people from Tiversa have discussions about the meeting?***" A. "***Yeah. I mean, we -- Bob spoke to me about next steps on the way home.***" Q. "***And what were the next steps?*** …" A. "***… Bob had indicated to me that the files needed to have spread on them, you know, basically look for them and see if they are available at other IP addresses, and if they're not, make them appear to have -- you know, be at different IP addresses.***") (emphasis added); (A. ***"Yes. That was the purpose of the meeting, was to clarify the – how I put the data together, how it would correspond with the list and the actual file."***) (emphasis added); (BY MR. SHERMAN: Q. ***"You testified that the purpose of the meeting was to discuss the information provided pursuant to the CID; is that correct?"*** A. ***"Yes."*** Q. ***"And do you recall who was at the meeting?"*** A. ***"There were multiple people. I mean, I don't – I don't remember specific – I do remember Alain was there."*** Q. ***"Alain who?"*** A. ***"Alain Sheer."***) (emphasis added).

59. The Commission's interest in LabMD stems from a study conducted by Dr. Eric Johnson ("Johnson"), then at Dartmouth College ("Dartmouth") and now at Vanderbilt University, "Data Hemorrhages in the Health-Care Sector," (CX 0382) and the 2009 testimony of Robert Boback before Congress – in both of these sources, the 1718 File was used as an example of a serious data breach. (RX 0403 (E. Johnson emails and article re: data hemorrhaging)); (CX 0721 (Johnson, Dep. at 68-69); (CX 0703 (Boback, Dep. at 156)).

60. Commission staff reached out to Dr. Johnson in February, 2009, and asked for a copy of the data hemorrhaging report and Dr. Johnson complied by sending them a copy. (RX 403 (E. Johnson emails and article re: data hemorrhaging)); (Johnson, Tr. 784).

61. Dr. Johnson's work largely focused on inadvertent sharing via P2P networks

because these networks were used to share music, videos and pictures coupled with the fact that there is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); RX 524 (Hill, Dep. at 149)).

62. In or around January 2008, Tiversa was a research partner to Dr. Johnson and Dartmouth College in a federally-funded study of data security in the health care industry. (Johnson, Tr. at 802-804); (Daugherty, Tr. at 979-985); (Tr. at 56-58 (opening statement)).

63. Tiversa aided Dartmouth's research by obtaining business-related records, including records containing sensitive patient information belonging to health care providers, found on P2P networks and provided this information to Dartmouth for its "Data Hemorrhages" article. (Johnson, Tr. 753-755; CX 0872 (Gormley, Dep. at 55-57)).

64. Complaint Counsel has not introduced any evidence that Tiversa, Johnson or Dartmouth had permission from any person, whether listed on the 1718 File or not, to obtain or disclose PHI as required by HIPAA. (Tr. 1-1486); (CX 0001 – CX 0878).

65. In January, 2008, Tiversa, using its patented technology, conducted searches on P2P networks using Dartmouth's search terms. (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 000010)).

66. Although LabMD's 1718 File is included and discussed in Dartmouth's "Data Hemorrhages" article, Dartmouth did not obtain the 1718 File using its search terms combined with Tiversa's technology. (Johnson, Tr. 772-780); (CX 0872 (Gormley, Dep. at 98-102)).

67. In April, 2008, months after Tiversa had concluded searching using Dartmouth's search terms, Johnson requested that Gormley provide him with more recently found information that would help "spice up" and "boost the impact" of his "Data Hemorrhages" article. (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 000010); (CX 0872 (Gormley, Dep. at

69-71)); (RX 483 (Emails between C. Gormley and E. Johnson Re: WSJ article); (Johnson, Tr. 772-774)).

68. The 1718 File was provided to Dartmouth as a result of Johnson's request to "spice up" and "boost the impact" of his report. (CX 0872 (Gormley, Dep. at 103); (Johnson, Tr. 779-780)).

69. Neither Tiversa nor Johnson nor Dartmouth had permission from any person listed in the 1718 File to disclose or obtain their PHI as required by HIPAA. (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5)).

70. In May 2008, Tiversa began contacting LabMD to purchase its remediation services, including sending LabMD a Tiversa Incident Response Services Agreement describing the fee schedule, payment terms, and services that would be provided – these contacts continued from mid-May through mid-July. (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (CX 0021 (Tiversa Incident Response Services Agreement); (Daugherty, Tr. 985-987)).

71. It was not until LabMD instructed Tiversa to direct any further communications to LabMD's lawyer that Tiversa ceased to press LabMD to purchase its services. (RX 059 (Email between Boyle and Tiversa re: breach); (Daugherty, Tr. at 988-990)).

72. The Chairman of the United States House Oversight and Government Affairs Committee ("OGR") commenced an investigation of Tiversa over a period of months in 2014,

also exploring FTC's relationship with Tiversa. (RX 542 (June 11, 2014 OGR Letter from Issa to Ramirez); (RX 543 (December 1, 2014 OGR Letter from Issa to Ramirez)).[3]

73. OGR issued a report dated January 2, 2015 that was embargoed until after Wallace testified in open court on May 5, 2015. (RX 644 ((STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA), *available at* http://www.scribd.com/doc/265820770/2015-01-02-Staff-Report-for-Rep-Issa-Re-Tiversa#scribd (last visited Aug. 9, 2015)).

74. The Staff Investigative Report from OGR makes many notable claims apparently based on documentary evidence supporting Wallace's testimony, including the following:

- Phone records and emails subpoenaed from FTC show a working relationship between Commission Staff and Tiversa beginning in 2007, as Wallace testified. ((RX 644 ((STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56-59) (citations omitted); (Wallace, Tr. 1346-1349)).
- The Report claims that in October, 2007, Boback provided FTC with documents. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).

[3] RX 542 and RX 543 were admitted into evidence by this Court for notices purposes only on February 12, 2015.

- Wallace testified to a meeting in August 2009 between Tiversa and FTC that led Boback to demand evidence of "spread." (Wallace, Tr. 1385) (Q. "Mr. Wallace, have you ever traveled to Washington, D.C. to meet with the FTC?" A. "Yes." Q. "When did you do that?" A. "I would say it would have been -- ***it would have been after the CID was issued [in July-August 2009]***, but I'm not sure of the exact date." Q. "Would it also have been after the list of companies was provided pursuant to the CID?" A. "***Yes. That was the purpose of the meeting, was to clarify the – how I put the data together, how it would correspond with the list and the actual file.***") (emphasis added); (Wallace, Tr. 1386 (BY MR. SHERMAN: Q. "You testified that the purpose of the meeting was to discuss the information provided pursuant to the CID; is that correct?" A. "Yes." Q. "And do you recall who was at the meeting?" A. "There were multiple people. I mean, I don't – I don't remember specific – ***I do remember Alain was there." Q. "Alain who?" A. "Alain Sheer."***) (emphasis added); (Wallace, Tr. 1387-1388) (Q. "Who traveled to D.C. [to meet with Alain Sheer and FTC] from Tiversa?" A. "Bob Boback was driving. I was in the car, Anju Chopra and Keith Tagliaferri." ***Q. "Following the meeting, did the people from Tiversa have discussions about the meeting?" A. "Yeah. I mean, we -- Bob spoke to me about next steps on the way home."*** Q. ***"And what were the next steps? …"*** A. "… ***Bob had indicated to me that the files needed to have spread on them, you know, basically look for them and see if they are available at other IP addresses, and if they're not, make them appear to have -- you know, be at different IP addresses.***") (emphasis added).

- OGR's Staff Investigation Report also claims a meeting occurred in August 2007 between FTC and Tiversa. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).
- OGR's Staff Investigation Report reproduces emails that purport to show Tiversa/Boback used advanced knowledge of FTC regulatory action for its own commercial gain, working with Lifelock to solicit business from companies that would be contacted by FTC. (RX 644 (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 56) (citations omitted)).
- OGR's Staff Investigation Report speculates that Tiversa could not have done so without some sort of inside knowledge of pre-decisional, non-public information. (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 52, 56, 62, 67) (citations omitted)).
- OGR's Staff Investigation Report claims FTC supposedly admitted in a briefing that the use of Tiversa's information was "unusual relative to standard agency operating procedures for enforcement measures," and that it relied heavily on Tiversa's "credible" reputation in "self-verifying" the information it had provided.

(RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 61) (citations omitted)).

- Wallace testified that Tiversa's Marine One claims were false and fabricated (Wallace, Tr. 1453-1454), and OGR's Staff Investigation Report makes similar claims consistent with Wallace's testimony.

  (RX 644 (STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 113th Cong., Tiversa, Inc.: White Knight Or High-Tech Protection Racket? (2015) (PREPARED FOR CHAIRMAN DARRELL E. ISSA) 16-18) (citations omitted)).

75. FTC was aware Tiversa had a clear and direct economic interest in FTC action against the companies it turned over for enforcement action. (CX 0679 (Ex. 5 (Dissenting Statement of FTC Comm'r J. Thomas Rosch, FTC File No. 1023099 (June 21, 2012)).

72. Shortly after the 2007 Congressional testimony concerning file sharing over P2P networks at which Boback and FTC Commissioner Engle testified, FTC began having frequent meetings with Tiversa to discuss its technology and the type of information that could be found on P2P networks. (Wallace, Tr. 1347-1350).

73. FTC personnel travelled to Tiversa's offices in Pittsburgh to get a demonstration of the technology. (Wallace, Tr. 1351).

74. FTC began requesting information from Tiversa that met a certain threshold which consisted of personally identifiable information exposed for greater than 100 people. (Wallace, Tr. 1562).

75. In 2009, the FTC and Tiversa agreed that a CID would be served on the Privacy Institute to funnel information from Tiversa to FTC. (RX 525 (Kaufman, Dep. at 20)).

76. The Privacy Institute was the company established to accomplish this. (Wallace, Tr. 1353); (CX 0703 (Boback, Dep. at 38-41)).

77. Wallace gathered the information and prepared the list of companies to be provided to FTC in response to the CID that the FTC served on the Privacy Institute. (Wallace, Tr. 1353-1354).

78. The list Wallace provided came from Tiversa's incident response case spreadsheet which Tiversa salespeople, including Boback, would use to sell Tiversa's remediation services to companies whose information Tiversa had discovered via P2P networks. (Wallace, Tr. 1359).

79. Boback provided the FTC with the list in response to the CID to the Privacy Institute as a way to get the companies contacted by the FTC to purchase Tiversa's services. (Wallace, Tr. 1352-1353).

69. The IP address listed on exhibit CX 0307 –64.190.82.42– is LabMD's IP address. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1353-1354)).

70. Tiversa later provided CX 0019 to FTC pursuant to a subpoena served upon Tiversa in conjunction with Mr. Boback's deposition. (CX 0541 (Boback, Dep. at 22-23)).

71. Wallace provided Boback with a copy of CX 0019 within 30 days of Boback's deposition. (CX 0541 (Boback, Dep. at 22-23)).

72. At Boback's direction Wallace created CX 0019 to demonstrate spread of the 1718 File to other IP addresses, and to establish that the 1718 File had not been found and taken from LabMD's IP address. (Wallace, Tr. 1380-1385).

73. The 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

74. It was not uncommon for Boback to retaliate against those who refused to purchase Tiversa's services. Boback instructed Wallace to make sure LabMD's name was at the top of the list provided to FTC. (Wallace, Tr. 1364-1366).

75. Despite Boback's testimony that Tiversa "responded to the civil investigative demand exactly to the letter," (CX 0703 (Boback, Dep. at 143)), some of Tiversa's clients who fit the criteria set out by the CID were omitted from the list. (Wallace, Tr. 1362-1363).

76. Complaint Counsel has declared it will not rely on Boback's testimony or CX 0019. (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Complaint Counsel's Opposition to Motion to Admit Select Exhibits, at 10, n.11 (June 24, 2015); (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Complaint Counsel's Response to Respondent's Motion to Refer Tiversa, Inc., Tiversa Holding Corp., and Robert Boback, at 2, n.1 (July 1, 2015)) ("As set forth in Complaint Counsel's Opposition to Respondent's Motion to Admit Select Exhibits, Complaint Counsel does not intend to cite to CX0019 or Mr. Boback's testimony in its proposed findings of fact. Nor does Complaint Counsel intend to cite to expert conclusions predicated on CX 0019 or Mr. Boback's testimony.") (citation omitted).

77. In 2009, FTC met with Tiversa to discuss the documents Tiversa provided to the Privacy Institute in response to the Civil Investigative Demand that FTC and Tiversa agreed would be served upon the Privacy Institute. (CX 0703 (Boback, Dep. at 140-142); (RX 525 (Kaufman, Dep. at 20)).

78. FTC first contacted LabMD about its investigation of LabMD in January 2010 with a telephone call to LabMD by Mr. Alain Sheer ("Sheer") and a subsequent eleven (11) page letter. (Daugherty, Tr. 992-994).

79. Mr. Daugherty instructed his employees to gather all documentation requested by the letter and provide it to FTC. (Daugherty, Tr. 996-997).

80. As a result of the Commission's collaboration with Tiversa, the Commission issued a February 22, 2010, press release titled "Widespread Data Breaches Uncovered by FTC Probe." (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

81. The Commission stated: "'we found health-related information, financial records, and drivers' license and social security numbers--the kind of information that could lead to identity theft…'" and that it had "notified almost 100 organizations that personal information, including sensitive data about customers and/or employees, ha[d] been shared from the organizations' computer networks." (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

82. The information "found" by the Commission was actually given to it by Tiversa. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (Wallace, Tr. 1358-1362); (CX 0703 (Boback, Dep. at 141-142)).

83. Over the next 18 months there were a series of resubmissions by LabMD to the FTC as well as phone calls and meetings about whether the information submitted was responsive and sufficient. (Daugherty, Tr. 997-1001); (CX 0443 (LabMD Access Letter Response by Philippa Ellis); (CX 0444 (LabMD Access Letter Response by Philippa Ellis); (CX 0445 (LabMD Access Letter Response by Philippa Ellis); (CX 0446 (LabMD Access Letter Response by Philippa Ellis); (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld);

(CX 0448 (LabMD Access Letter Response by Dana Rosenfeld); (CX 0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions)).

84. In or around August or September 2011, LabMD was presented with a Consent Decree that LabMD refused to sign. (Daugherty, Tr. 1001-1002).

85. In August, 2013, Complaint Counsel filed a Complaint and Notice Order against LabMD. (Complaint, at 12 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

D. **LabMD's Data Security**.

86. There is no perfect data security. (CX 0721 (Johnson, Dep. at 25, 38, 90); RX 524 (Hill, Dep. at 149); (Order Denying Respondent LabMD's Motion to Dismiss, at 18-19 (Jan. 16, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (last accessed Aug. 9, 2015)).

87. According to Complaint Counsel and its expert Dr. Raquel Hill ("Hill" or "Dr. Hill"), LabMD's data security was unreasonable because Respondent engaged in a number of practices between 2005 and July, 2010 that taken together failed to provide reasonable and appropriate security for personal information on its computer networks. (Complaint, at 3 ¶ 10 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

88. Dr. Hill testified that she did not consider FTC standards and guidelines for data security in determining whether LabMD's data security during the Relevant Period met those standards. (Hill, Tr. 230-231).

89. In reviewing data security standards and guidelines to assist in formulating her opinion in this case, Dr. Hill did not consider HIPAA guidelines or FTC data security standards. (Hill, Tr. 235-236); (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business

(Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)) ("A sound data security plan is built on 5 key principles: 1. Take stock. Know what personal information you have in your files and on your computers. 2. Scale down. Keep only what you need for your business. 3. Lock it. Protect the information that you keep. 4. Pitch it. Properly dispose of what you no longer need. 5. Plan ahead. Create a plan to respond to security incidents.").

90. FTC's "guide" entitled Protecting Personal Information: A Guide to Business was not published in the Federal Register and was issued in November 2011, more than one year after FTC commenced its inquisition in this case. (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)).

92. During the Relevant Time the LabMD Employee Handbook advised employees of the importance of compliance with HIPAA and the "Privacy of Protected Information" and that disclosure of PHI could result in termination. (CX 0001 (LabMD Employee Handbook (rev. June 2004), at 6); (CX 0002 (LabMD Employee Handbook (rev. Mar. 2008), at 5-6)).

93. During the Relevant Time each and every LabMD employee signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement indicating that they had received the LabMD handbook and had an understanding of and would comply with LabMD's ethics policy and employment policy. (CX 0130 (LabMD Employee Handbook)).

94. At all times relevant LabMD's Employee Handbook informed employees that LabMD computers were to be used for company purposes only and prohibited personal internet

or email usage. (CX 0001 (LabMD Employee Handbook (rev. June 2004), at 7); (CX 0002 (LabMD Employee Handbook (rev. Mar. 2008), at 7)).

95. Effective January 2003, LabMD had in place a Compliance Program for all employees which set forth the Policies and Standards of Conduct regarding Compliance Protocols, laws, statutes, regulations, rules and guidelines under which LabMD operated for the period 2003–2008. (CX 0005 (LabMD Compliance Program, at 1–10)).

96. Effective the Fourth Fiscal Quarter 2001, LabMD had the following Policies in practice: Data Backup Policy and Employee User Account Policy. (CX 0006 (LabMD Policy Manual, at 10, 12); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

97. Effective the Second Fiscal Quarter 2002, LabMD had the following Policies in practice: Desktop Monitoring Policy; Document Backup Software Policy; Monitor Security Software Settings and Operating System Updates Policy; Password Policy; Risk Assessment and Vulnerability Policy; Security Assignment and Accountability Policy; Server Monitoring Policy; and Software Monitoring Policy. (CX 0006 (LabMD Policy Manual, at 11, 13–19); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

98. Effective the Second and Fourth Fiscal Quarters (FQ) 2003, LabMD had the following Policies in practice: Client User Account Policy (Second FQ) and Audit Security Operations and Internet Connectivity Policy (Fourth FQ). (CX 0006 (LabMD Policy Manual, at 8–9); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

99. Effective the Second Fiscal Quarter 2004, LabMD had the following Policy in practice: Acceptable Use and Security Policy. (CX 0006 (LabMD Policy Manual, at 3–7); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

100. LabMD informed all employees of "new policies that may be added to the following general employment policies and guidelines" contained in the LabMD employee handbook. (CX0001 (LabMD Employee Handbook, at 2)).

101. "Our Ethics Policy is included in the employee handbook and you will learn more about safety, privacy, security and other policies in the next several weeks of your orientation." (CX 0001 (LabMD Employee Handbook, at 2)).

102. LabMD's Mission Statement for the period 2004–2008 was as follows: "Using all reasonable means, LabMD has the intent to be fully compliant with the rules, laws and guidelines regulating its business." (CX 0001 (LabMD Employee Handbook, at 3)).

103. LabMD's Purpose for the period 2004–2008 was as follows: "LabMD, Inc. seeks to operate within the guidelines and intent of laws, statutes and regulations governing medical laboratories. In keeping employees and business associates educated, informed and trained, we can be watchful of our lab, business and billing practices in an effort to move responsibility for compliance to all levels and all departments of our organization. In short we intend to make compliance everyone's job. This compliance program establishes a formal structure to monitor, detect, respond to, and correct violations of applicable federal, state and local laws, and regulations, as well as violations of the Standards of conduct [*sic*] and LabMD policies. Our objective is to make compliance a business competency shared, valued and practiced by all individuals within LabMD. LabMD shall provide mechanisms and resources broad enough to accomplish this objective. This Corporate Compliance Program applies to all officer [*sic*], employees, business associates and agents of LabMD, Inc." (CX 0001 (LabMD Employee Handbook, at 3)).

104. LabMD's Statement of Purpose and Ethics Policy for the period 2004-2008 required total compliance at all times by all employees with all applicable federal, state, and local laws, regulations and policies. (CX 0001 (LabMD Employee Handbook), at 1-23)).

105. LabMD's Corporate Compliance Program, Standards of Conduct, and Policies for the period 2004-2008 required total compliance at all times by all employees with said Program, Standards, and Policies. (CX 0001 (LabMD Employee Handbook, at 1-23)).

106. LabMD's Confidentiality and Trade Secrets Policy for the period 2004-2008 was as follows: "In the course of your work, you may have access to confidential information regarding LabMD, its suppliers, customers, operations methods, current or potential products or services and software used at LabMD. It is one of your most serious responsibilities that you in no way reveal or divulge any such information and that you use information only in the performance of your duties, as certain information could be used by competitors. . . . Removal and/or possession [of LabMD information] without . . . authorization is prohibited and subject to disciplinary action up to and including termination. . . ." (CX 0001 (LabMD Employee Handbook, at 5)).

107. LabMD's Privacy of Protected Health Information (PHI) Policy for the period 2004-2008 was as follows: "[HIPAA] made it illegal for any person in health care to share an individual's protected health care information [PHI] with anyone other than for the specific reasons of treatment, payment or health care operations. Because of this, LabMD has taken specific measures to ensure our compliance with this law. As an employee you are required to share information only with authorized individuals and only for specific, authorized reasons. You will learn more about how that affects your job specifically. Any person providing PHI to another person that is unauthorized will be disciplined up to and including termination."

(CX 0001 (LabMD Employee Handbook, at 6)).

108. LabMD's Policy regarding employee use of LabMD on–site computers for the period 2004–2008 was as follows: "***Personal internet or e–mail usage in the office is prohibited. This [P]olicy stands at all times, even when an employee is on a lunch period. Computers in the office are property of LabMD and should only be used for company related reasons.***" (CX 0001 (LabMD Employee Handbook, at 7)) (emphasis added)).

109. LabMD's Policy regarding LabMD property during the 2004-2008 time period was, in relevant part, as follows: "computers and all office equipment are LabMD's property and must be maintained according to LabMD's standards, rules, and regulations." (CX 0001 (LabMD Employee Handbook, at 9)).

110. LabMD's Policy regarding Employee Health Records during the 2004-2008 time period was as follows: "Health/medical records are not included in your personnel file. These records are confidential. LabMD will safeguard them from disclosure and will divulge such information only as allowed or required by law and in accordance with HIPAA Privacy guidelines." (CX 0001 (LabMD Employee Handbook, at 12)).

111. Effective the Second Fiscal Quarter 2008, LabMD had the following Policies in practice: PC System Setup To Prevent Downloading Files From Internet Policy; Prohibit Use Of File–Sharing Software Policy; and Security Incident Response Plan. (CX 0006 (LabMD Policy Manual, at 20-22); (CX 0444 (LabMD Access Letter Response by Philippa Ellis)).

112. LabMD informed all employees of "new policies that may be added to the following general employment policies and guidelines" contained in the LabMD employee handbook. (CX 0002 (LabMD Employee Handbook, at 2)).

113. LabMD's Mission Statement for the period 2008-2010 was as follows: "Using all reasonable means, LabMD has the intent to be fully compliant with the rules, laws and guidelines regulating its business." (CX0002 (LabMD Employee Handbook, at 3)).

114. LabMD's Purpose for the period 2008-2010 was identical to its Purpose for the 2004-2008 time period. (CX 0002 (LabMD Employee Handbook, at 3)).

115. LabMD's Statement of Purpose and Ethics Policy for the period 2008-2010 required total compliance at all times by all employees with all applicable federal, state, and local laws, regulations and policies. (CX 0002 (LabMD Employee Handbook, at 1-22)).

116. LabMD's Corporate Compliance Program, Standards of Conduct, and Policies for the period 2004-2008 required total compliance at all times by all employees with said Program, Standards, and Policies. (CX 0002 (LabMD Employee Handbook, at 1-22)).

117. LabMD's Privacy of Protected Health Information (PHI) Policy for the period 2008-2010 was as follows: "[HIPAA] made it illegal for any person in health care to share an individual's protected health care information [PHI] with anyone other than for the specific reasons of treatment, payment or health care operations. Because of this, LabMD has taken specific measures to ensure our compliance with this law. As an employee you are required to share information only with authorized individuals and only for specific, authorized reasons. You will learn more about how that affects your job specifically. Any person providing PHI to another person that is unauthorized will be disciplined up to and including termination." (CX 0002 (LabMD Employee Handbook, at 6)).

118. LabMD's Policy regarding employee use of LabMD on-site computers for the period 2008-2010 was as follows: "Personal internet or e–mail usage in the office is prohibited. This [P]olicy stands at all times, even when an employee is on a lunch period. Computers in the

office are property of LabMD and should only be used for company related reasons." (CX 0002 (LabMD Employee Handbook, at 7)).

119. LabMD's Policy regarding LabMD property during the 2008-2010 time period was, in relevant part, as follows: "[C]omputers and all office equipment are LabMD's property and must be maintained according to LabMD's standards, rules, and regulations." (CX 0002 (LabMD Employee Handbook, at 9)).

120. Effective June 1, 2010, LabMD utilized a completed Computer Hardware, Software and Data Usage and Security Policy Manual, which documented LabMD's existing policies and incorporated ongoing data security policies. (RX 0074 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual, at 1-32)).

121. For the period 2001-2010, LabMD utilized in practice the following data security policies for evaluating, identifying and addressing confidentiality and data security measures, safeguards, and risks: (1) Acceptable Use and Security Policy; (2) Assessment – Audit Policy; (3) Audit Security Operations and Internet Connectivity Policy; (4) Client User Account Policy; (5) Data Backup Policy; (6) Desktop Monitoring Policy; (7) Document Backup Software Policy; (8) Education and Training – Anti–Virus and Anti–Spyware Applications; (9) Education and Training – Instruction for Closing Network Connections; (10) Education and Training – Instruction of P2P Applications; (11) Employee User Account Policy; (12) Monitor Security Software Settings and Operating System Updates Policy; (13) Password Policy; (14) PC System Setup To Prevent Downloading Files From Internet Policy; (15) Prohibit Use of File–Sharing Software Policy; (16) Risk Assessment and Vulnerability Policy; (17) Security Assignment and Accountability Policy; (18) Security Incident Response Plan; (19) Server Monitoring Policy; and (20) Software Monitoring Policy. (CX 0445 (LabMD Access Letter Response by Philippa Ellis);

(RX 074 (LabMD Computer Hardware and Security Manual, at 1-32); (CX 0006 (LabMD Policy Manual, at 1-22); (CX 0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual at 2, 11-32)).

122. Information in LabMD's Employee Handbook qualifies as the written policies of the company. (Hill, Tr. 289).

123. In 2001, LabMD hired an IT consulting firm, ITrain Tech, to design and set up LabMD's IT system at its Savannah, Georgia location. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

124. For LabMD, ITrain Tech focused on the design and implementation of IT networks and PC setup projects primarily for small businesses and assisted with network design, including the purchase and installation of software and firewalls. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

125. ITrain Tech was under contract with LabMD through August 2004 and remained on call as necessary thereafter. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

126. LabMD IT employee Jeremy Dooley ("Dooley") started with the company in 2004 and ended his employment in December, 2006. He testified that during his tenure LabMD had firewalls installed to protect against intrusions, as well as antivirus software. (CX 0711 (Dooley, Dep. at 31, 71-72)).

127. Dooley signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement on March 10, 2005. (CX 0130 (LabMD Employee Handbook, at 003835)); (CX 0711, (Dooley, Dep. at 143)).

128. Dooley's first title and responsibilities were as the communication coordinator assigned with calling insurance companies to verify benefits. (CX 0711 (Dooley, Dep. at 13)).

129. Later Dooley joined the technical support team and would go around and repair computers. (CX 0711 (Dooley, Dep. at 15- 16)).

130. Lytec was the billing software used by LabMD. (CX 0711 (Dooley, Dep. at 52-53)).

131. LabSoft was the laboratory software used by LabMD. (CX 0711 (Dooley, Dep. at 125)).

132. At that time, LabMD had firewalls installed to protect against intrusions and also installed antivirus software. (CX 0711 (Dooley, Dep. at 31, 71-72)).

133. Both the lab software and the billing software had separate firewall routers. (CX 0711 (Dooley, Dep. at 24)).

134. Security risks and vulnerabilities were assessed by Automated PC Technologies ("APT"), an outside contractor. (CX 0711 (Dooley, Dep. at 38-39)).

135. Allen Truett ("Truett") started APT in 1996 – APT provided technology consulting services to small and medium-size businesses. (CX 0731 (Truett, Dep. at 17-18)).

136. APT began providing services to LabMD in 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX 0731 (Truett, Dep. at 25, 72-73)).

137. APT consulted with and made recommendations to LabMD with respect to installing and maintaining firewalls and antivirus software to mitigate threats and risks for medical organizations like LabMD to prevent information on its secure internal network from being accessed from the outside. (CX 0731 (Truett, Dep. at 45-46)).

138. APT performed network diagnostics by looking at network traffic. (CX 0711 (Dooley, Dep. at 52); (CX 0731 (Truett, Dep. at 69)).

139. APT installed and managed antivirus software. (CX 0711 (Dooley, Dep. at 71-72); (CX 0731 (Truett, Dep. at 19)).

140. APT provided backup software and applied patches. (CX 0711 (Dooley, Dep. at 114); (CX 0731 (Truett, Dep. at 32)).

141. APT was an IT outsourcing company specializing in the medical field. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld)).

142. APT's start-up procedures for LabMD included an evaluation its antivirus and firewall systems. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld (Ex. 3)).

143. APT began evaluating LabMD's existing security features and providing backup services to LabMD, including identifying and remedying a problem with LabMD's server's virus scan on May 3, 2006. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld (Ex. 5)).

144. APT identified and resolved anti-virus program concerns at LabMD throughout 2006. (CX 0447 ((LabMD Access Letter Response by Dana Rosenfeld)).

145. After advising LabMD to install an additional firewall on May 6, 2006, APT obtained LabMD's authorization and delivered the new firewall for installation on May 12, 2006. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld (Ex. 5)).

146. APT implemented and tested all new upgrades during the period of August 2003 through March 2007 to ensure that equipment and software was functioning properly. (CX 0447 (LabMD Access Letter Response by Dana Rosenfeld (Ex. 4)).

147. APT installed a ZyWALL firewall application, which was specific to APT's medical clients for Internet security, and another firewall application for LabMD during the 2006-2008 time period. (CX 0731 (Truett, Dep. at 31, 33, 41)).

148. During the 2006-2008 time period, APT did work concerning the administration of servers and firewalls and "[i]nstallation of service packs and upgrade and software patches for PCs and servers." (CX 0731 (Truett, Dep. at 31-33)).

149. On May 12, 2006, APT delivered a ZyWALL 5 IPSec firewall to LabMD. (CX 0731 (Truett, Dep. at 60-61)).

150. During the period 2006-2008, LabMD installed and utilized Trend Micro antivirus software. (CX 0731 (Truett, Dep. at 89)).

151. During the period 2007-2008, LabMD had Veritas backup software on its servers. (CX 0724 (Maire, Dep. at 23)).

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

153. During the period 2007-2008, LabMD had a Windows firewall on its computer system. (CX 0724 (Maire, Dep. at 97)).

154. LabMD's computer data security was reasonable and appropriate for the period 2007–2008. (CX 0724 (Maire, Dep. at 89)).

155. LabMD had a firewall intrusion-prevention system in place for the period 2007-2008. (CX 0724 (Maire, Dep. at 91)).

156. LabMD had in place the Zywall firewall hardware and other security measures, including Internet access restrictions for non-managerial employees, as well as TrendMicro anti-virus software and stratified profile setups, which limited the ability of employees to modify

computer settings and which were organized at three different levels: “Admin,” “Local Admin,” and “User level,” for administrators, managers and line-level employee users). (CX 0704-A (Boyle, Dep. at 49-55)).

157. At the time, IT support services were provided by APT and internal staffing, and LabMD IT personnel implemented network upgrades and maintained the day-to-day monitoring and functioning of the network. (CX 0704-A (Boyle, Dep. at 12, 39, 44-48)).

158. There were layers of authentication with the initial layer being the Windows network and the others being a layer for the billing software and a layer for the lab software. (CX 0711 (Dooley, Dep. at 125)).

159. LabMD placed restrictions on employees’ access to information through the authentication layers, usernames and passwords. (CX 0711 (Dooley, Dep. at 124-127)).

160. Only certain individuals were given administrator user profiles which gave them the ability to install applications. Most employees were given standard user profiles. (CX 0711 (Dooley, Dep. at 47-49)).

161. Dooley had no concerns about the security of LabMD’s network. (CX 0711 (Dooley, Dep. at 151-152)).

162. There were no concerns about the security of LabMD’s network either specifically or generally, and there were no incidents of unauthorized access. (CX 0731 (Truett, Dep. at 126-127)).

163. Outside contractors were brought in proactively to identify security issues. (CX 0711 (Dooley, Dep. at 152)).

164. Billing employee Nicotra Harris (“Harris”) was employed by LabMD from October 2006 through January 2013. (CX 0716 (Harris, Dep. at 11)).

165. Harris described her access to the Internet as limited to insurance companies' websites or otherwise being blocked. (CX 0716 (Harris, Dep. at 82-83)).

166. Harris testified that on a yearly basis LabMD employees received training on LabMD compliance standards, HIPAA compliance, and the limited use of computer systems, including the restricted use of the Internet and the prohibition against playing CDs or downloading of information from the Internet. (CX 0716 (Harris, Dep. at 62)).

167. Harris testified that LabMD had in place user names and passwords for billing department employee computers with separate and different user names and passwords for the Lytec billing system. (CX 0716 (Harris, Dep. at 67-68)).

168. Harris testified only billing personnel could access the Lytec billing system. (CX 0716 (Harris, Dep. at 75)).

169. Harris testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. (CX 0716 (Harris, Dep. at 72-74)).

170. Harris testified insurance aging reports were created and printed by the billing managers, and that the pages were divided amongst the billing department employees for the purpose of contacting insurance companies to collect unpaid balances – when they were finished using the portion of the report they had been given they would shred them. (CX 0716 (Harris, Dep. at 34-41)).

171. Harris testified that she had no knowledge of a breach of LabMD's system during her tenure. (CX 0716 (Harris, Dep. at 130-131)).

172. Billing employee [redacted] was employed by LabMD from 2007 through January 2009. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 13)).

173. [redacted] also testified to LabMD's security policies and practices including the shredding of the insurance aging reports. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 43, 45-47, 49-50, 54-55, 61-62, 65-66)).

174. [redacted] testified that she received HIPAA training by watching a video on privacy concerns and HIPAA violations. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 86)).

175. [redacted] testified that LabMD had in place user names and passwords for billing department employee computers and separate and different user names and passwords for the Lytec billing system as well as different user names and passwords for access to the LabSoft program. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 43, 45)).

176. [redacted] testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to bill denials of coverage for medically necessary tests. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 46-47)).

177. [redacted] testified insurance aging reports were created and printed by the billing managers and used for the purpose of contacting insurance companies to collect unpaid balances. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 49-50)).

178. [redacted] testified that when they were finished using the portion of the report they had been given they would shred them. (CX 0714-A (PUBLIC Deposition Transcript of Former LabMD Employee, at 54-55)).

179. LabMD billing employee Sandra Brown ("Brown") was the billing manager from May 2005 to May 2006. (CX 0706 (Brown, Dep. at 6-7)).

180. Brown testified that from 2006 through 2013 she worked from home doing billing from insurance aging reports. (CX 0706 (Brown, Dep. at 7)).

181. Brown testified that LabMD limited internet access to the insurance company web sites and only managers had access to Microsoft Outlook emails. (CX 0706 (Brown, Dep. at 115, 121)).

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

183. Brown testified that it was necessary for billing personnel to have access to LabSoft in order to do their jobs. They would use this information to send information to insurance companies if they asked for medical records and for an appeals request. (CX 0706 (Brown, Dep. at 117-118, 153)).

184. Brown testified that Insurance aging report pages were shredded. (CX 0706 (Brown, Dep. at 143-144)).

185. Billing employee Patricia Gilbreth ("Gilbreth"), who later became a billing manager, was employed from 2007 to 2013 at LabMD. (CX 0715-A (Gilbreth, Dep. at 77-78)).

186. Gilbreth testified there was annual training at LabMD about HIPAA and protecting information. (CX 0715-A (Gilbreth, Dep. at 77-78)).

187. Gilbreth testified that she conducted training for new billing department employees which included the employee handbook and security handbook. (CX 0715-A (Gilbreth, Dep. at 81-83)).

188. Gilbreth testified that the ability to create or print an insurance aging report was limited to a few people in the billing department. (CX 0715-A (Gilbreth, Dep. at 33-35)).

189. Gilbreth testified the aging reports were shredded. (CX 0715-A (Gilbreth, Dep. at 14-16)).

190. Gilbreth testified there were restrictions on access to the internet and there was a prohibition in the employee handbook against downloading from the internet. (CX 0715-A (Gilbreth, Dep. at 63-65)).

191. Gilbreth testified she was familiar with portions of the LabMd policy manual and the "IT security handbook" which was updated periodically. (CX 0715-A (Gilbreth, Dep. at 85-86); (CX 0006 (LabMD Policy Manual)).

192. Gilbreth testified there was a policy against personal email accounts. (CX 0715-A (Gilbreth, Dep. at 57)).

193. Gilbreth testified that she considered the downloading of LimeWire on Woodson's computer a company security policy violation. (CX 0715-A (Gilbreth, Dep. at 67-68)).

194. Gilbreth testified she had no concerns and knew of no other employee who had concerns about LabMD's information security policies and procedures. (CX 0715-A (Gilbreth, Dep. at 67)).

195. John Boyle ("Boyle") was employed as LabMD's Vice President of Operations and General Manager from November 2006 to August 2013. (CX 0704-A (Boyle, Dep. at 7-8)).

196. Boyle brought to LabMD an enormous amount of knowledge and experience in information technology and data security within the medical laboratory industry: prior to joining LabMD Boyle worked for Cyto Diagnostics as a lab technician creating slides for urine samples,

a DNA analysis lab technician creating computer generated reports and was promoted to team lead responsible for the entire process from receiving and processing the samples, staffing, writing and implementing policies and procedures and processes to qualify. (CX 0704-A (Boyle, Dep. at 92-96)).

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

198. Boyle was then promoted to the position of client relations interface manager where he interacted with the internal clients, the departments, and external clients, the physicians. (CX 0704-A (Boyle, Dep. at 101-102)).

199. Later Boyle was promoted to the position of operations business analyst where he worked daily with the IT department on applications and structure to develop working product for segments of operations. (CX 0704-A (Boyle, Dep. at 103-104)).

200. Boyle was then moved into the IT department where he became the business analyst/information planning manager where part of his duties were to choose and implement a new billing and laboratory system giving consideration to that new system’s ability to receive and process information electronically. (CX 0704-A (Boyle, Dep. at 105-109)).

201. At that time Robert Hyer ("Hyer") was director of IT at UroCor, and was a mentor to Boyle – both worked together at UroCor in choosing the new billing and laboratory systems for UroCor. (CX 0719 (Hyer, Dep. at 17); (CX 0704-A (Boyle, Dep. at 110-111)).

202. When UroCor was purchased by DIANON and as a result Boyle became the Oklahoma City facility laboratory manager responsible for lab management over all departments in the facility while working with the IT departments for LabCorp and DIANON which involved planning, design review, coordination between IT departments and clients and interfaces. (CX 0704-A (Boyle, Dep. at 112-113)).

203. From 2003-2006, Boyle was the director of operations for DIANON in 2003 through 2006 at which time external and internal transfers of protected health information were mostly conducted electronically and Boyle had the responsibility to ensure that those transfers were secure. (CX 0704-A (Boyle, Dep. at 114-118)).

204. When Boyle joined LabMD in November of 2006 he described LabMD's system as being designed from the outside in making it efficient for the physicians to use. (CX 0704-A (Boyle, Dep. at 123-125)).

205. Boyle found the design of the transfer of information from clients to LabMD and the internal transfer of information within LabMD to be efficient and secure. (CX 0704-A (Boyle, Dep. at 125)).

206. Information came to LabMD from physicians through a secure connection. (CX 0704-A (Boyle, Dep. at 13)).

207. Boyle assumed oversight of compliance training for LabMD employees. LabMD's existing policies already prohibited employees, other than certain authorized IT

personnel, from downloading programs or applications from the Internet. (CX 0704-A (Boyle, Dep. at 39-48, 54-55, 68 -71)).

208. When Boyle arrived LabMD's IT department was flat – there were no supervisors. (CX 0704-A (Boyle, Dep. at 52-53)).

209. IT personnel (including Curt Kaloustian, Alison Simmons and Chris Maire) reported directly to Boyle. (CX 0704-A (Boyle, Dep. at 12)).

210. Upon Boyle's arrival he found that LabMD had in place the Zywall firewall application installed by APT which was specific to APT's medical clients for Internet security; along with security measures, including Internet access restrictions for non-managerial employees, TrendMicro anti-virus software and stratified profile setups, which limited the ability of employees to modify computer settings (there were three different levels: "Admin," "Local Admin," and "User level," for administrators, managers and line-level employee users). (CX 0731 (Truett, Dep. at 31, 33, 41); (CX 0704-A (Boyle, Dep. at 49-55)).

211. APT would regularly be on site at LabMD managing networking, servers, hardware and applications. (CX 0704-A (Boyle, Dep. at 47-48); (CX 0731 (Truett, Dep. at 32)).

212. IT support services were provided by APT and internal staffing, and LabMD IT personnel implemented network upgrades and maintained the day-to-day monitoring and functioning of the network. (CX 0704-A (Boyle, Dep. at 12, 39, 44-48)).

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

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

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

216. If a problem were reported or observed, LabMD's IT personnel would attend to it immediately, on site. (CX 0704-A (Boyle, Dep. at 39-48, 54-55, 68-71)).

217. On February 25, 2008, Rick Wallace entered LabMD's system without authorization and downloaded the 1718 File from a LabMD workstation that was running a P2P file sharing program. (Wallace, Tr. 1441).

218. Wallace entered LabMD's system without authorization and downloaded the 1718 File for Tiversa's financial benefit. (Wallace, Tr. 1344, 1360-1361, 1364).

219. At the time Wallace entered LabMD's system without authorization and downloaded the 1718 File on February 25, 2008, Georgia law provided as follows:

- **(a)** ***Computer theft.*** Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

  (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;

  (2) Obtaining property by any deceitful means or artful practice; or

(3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

- **(b)** ***Computer Trespass.*** Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

(1) Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;

(2) Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or

(3) Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

- **(c)** ***Computer Invasion of Privacy.*** Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.
- **(d)** ***Computer Forgery.*** Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had

created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

- **(e)** ***Computer Password Disclosure.*** Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.
- **(f)** ***Article not Exclusive.*** The provisions of this article shall not be construed to preclude the applicability of any other law which presently applies or may in the future apply to any transaction or course of conduct which violates this article.
- **(g)** ***Civil Relief; Damages.***

  (1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits and victim expenditure.

(2) At the request of any party to an action brought pursuant to this Code section, the court shall by reasonable means conduct all legal proceedings in such a way as to protect the secrecy and security of any computer, computer network, data, or computer program involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(3) The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(4) A civil action under this Code section must be brought within four years after the violation is discovered or by exercise of reasonable diligence should have been discovered. For purposes of this article, a continuing violation of any one subsection of this Code section by any person constitutes a single violation by such person.

- **(h)** ***Criminal Penalties.***

  (1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.

  (2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

(Off. Code of Ga. Ann. § 16-9-93 (2008) (Georgia Computer Crimes Statute), *available at* http://law.justia.com/codes/georgia/2010/title-16/chapter-9/article-6/part-1/16-9-93 (last accessed Aug. 9, 2015).

220. At the time Wallace entered LabMD's system without authorization and downloaded the 1718 File, HIPAA prohibited Tiversa from obtaining or disclosing PHI of any individual without that person's express permission because LabMD was a covered entity under 42 U.S.C. § 1320d-9(b)(3). (42 U.S.C. § 1320d-6(a) & (b) (Wrongful disclosure of individually identifiable health information)).

218. "The FTC's Complaint in [this] Enforcement Action makes clear that LabMD was a 'health care provider' and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 12 ¶ 42)).

218. 42 U.S.C. § 1320d-6 (a) & (b) provide as follows:

- **(a) Offense**

  A person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) ***obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d–***

9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.

- **(b) Penalties**

A person described in subsection (a) of this section shall—(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and ***(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.***

(emphasis added).

221. There is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); (RX 524 (Hill, Dep. at 149)).

222. In May, 2008, Tiversa, through Boback, contacted LabMD alleging that the 1718 File had been found on the internet and offering "remediation" services. (RX 050 (Email between Boyle and Tiversa); (RX 051 (Email between Boyle and Tiversa); (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa) ([Boback to Boyle 15 May 2008] ("Per Rick's email below, it would require some time to get to that type of information which would need to be handled through our Incident Response Operation Team and would require a professional services arrangement. As I mentioned in my last email, there are many more necessary benefits to a proper investigation of the disclosure by our team."); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and

Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (CX 0021 (Tiversa Incident Response Services Agreement); (Daugherty, Tr. 979-993)).

223. This was after Tiversa had shared the 1718 File with Johnson and Dartmouth. (CX 0872 (Gormley, Dep. at 86-87)).

224. At all times relevant, Tiversa knew or should have known the 1718 File contained highly confidential information and that it was not authorized to obtain or disclose the 1718 File to any third party because Tiversa "found" the LabMD 1718 page document, and a Tiversa email dated April 17, 2008 categorizes how many social security numbers (SSNs) and other identifying information were in that file, which included information commonly known as PII and PHI. (CX 0872 (Gormley, Dep., at 81-83, 86-87)) ("[This is] an E-mail describing the contents of a file labeled subject, LabMD disclosure, categorizing how many social security numbers and other identifying information … [MR. SHERMAN:] So it's a possibility that the LabMD disclosure as it is called in the subject line of this E-mail was discovered as a result of searches that Tiversa was doing for other clients. [Mr. Gormley:] That's possible. Social security number would have been a term that we would have looked for. CIGNA would have been a term that we would have looked for because they were a client.") (discussing Gormley Dep. Ex. RX 5 (4/17/2008 Wallace email to Gormley – subject line of "LabMD disclosure")).

221. This type of information uncovered by Tiversa would be regularly shared with Tiversa's customers. (CX 0872 (Gormley, Dep. at 83, 86-87)).

222. After Tiversa contacted LabMD, and advised that the 1718 File had been downloaded via a P2P file sharing program, at Boyle's direction, LabMD IT employee Alison Simmons ("Simmons") searched all computers at LabMD for file sharing software. (CX 0704 (Boyle, Dep. at 57-66, 74-88); (CX 0149 (Screenshot: LabMD - Tiversa.zip WINRAR -

insuranceaging_6.05.071.pdf); (CX 0150 (Screenshot: C:\); (CX 0151 (Screenshot: C:\Program Files\LimeWire); (CX 0152 (Screenshot: LimeWire: My Shared Files); (CX 0153 (Screenshot: LabMD - Tiversa.zip WinRAR - LabMD folder); (CX 0154 (Screenshot: LimeWire Get Started); (CX 0155 (Screenshot: Start Menu: LimeWire); (CX 0156 (Screenshot: LimeWire: Options: Shared Folders); (CX 0157 (Screenshot: insuranceaging_6.05.071.pdf Properties)).

223. Simmons found no file sharing software on any other computer except for the billing manager Roz Woodson's computer. (CX 0730 (Simmons, Dep. at 10-11)).

224. Simmons removed the LimeWire file sharing program from Woodson's computer. (CX 0730 (Simmons, Dep. at 14-15)).

225. According to Simmons the billing department had a firewall and billing employees were prohibited from going to nonspecified web sites, except for those needed to perform their jobs. (CX 0730 (Simmons, Dep. at 16)).

226. Under Boyle's supervision and with his personal assistance, LabMD IT personnel Simmons and Jeff Martin ("Martin") immediately undertook a search of all other computers in the office and determined that no other LabMD computers contained either the LimeWire application or the 1718 File. (CX 0704-A (Boyle, Dep. at 57-64)).

227. To verify what LabMD had been told by Tiversa, Boyle instructed Simmons to search for the file on P2P networks from her home computer; Simmons searched for the file two hours on the day of the call from Tiversa and then once a week for a month or longer but was never able to find the 1718 file. (CX 730 (Simmons, Dep. at 17-18)).

228. As part of LabMD's investigation after the LimeWire discovery, Simmons, under Boyle's supervision, took a series of screenshots from the billing manager's computer and placed them on a CD, and the screenshots showed the date LimeWire files had been installed on the

billing manager's computer and the presence of the file, which Tiversa had told LabMD it had downloaded from a P2P file sharing site. (CX 0704-A (Boyle Dep. at 57-66, 74-88)); (CX 0149 (Screenshot: LabMD - Tiversa.zip WINRAR - insuranceaging_6.05.071.pdf); (CX 0150 (Screenshot: C:\); (CX 0151 (Screenshot: C:\Program Files\LimeWire); (CX 0152 (Screenshot: LimeWire: My Shared Files); (CX 0153 (Screenshot: LabMD - Tiversa.zip WinRAR - LabMD folder); (CX 0154 (Screenshot: LimeWire Get Started); (CX 0155 (Screenshot: Start Menu: LimeWire); (CX 0156 (Screenshot: LimeWire: Options: Shared Folders); (CX 0157 (Screenshot: insuranceaging_6.05.071.pdf Properties)).

229. Boyle assigned IT employee Simmons and later Martin to search P2P networks to find the 1718 file and they could not find the file on any P2P networks. (CX 0704-A (Boyle, Dep. at 63-64)).

230. Simmons was asked to interview Woodson and determine her knowledge of the program. Simmons concluded Woodson appeared to have no idea what the program was or whether she had shared files. (CX 0730 (Simmons, Dep. at 12, 93)).

231. According to Simmons no one was supposed to download anything without going through IT. (CX 0730 (Simmons, Dep. at 17)).

232. Woodson was terminated as a result of the P2P incident. (CX 0730 (Simmons, Dep. at 99- 100)).

233. From August 2008 until June 2010 John Boyle personally conducted walk arounds on a weekly basis, assisted by Hyer or another IT employee, such as Matt Bureau ("Bureau"). (CX 0704-A (Boyle, Dep. at 39-40, 130-31)).

234. LabMD routinely performed daily IT rounds to check on the data security status

of all computer systems. (RX 174 – RX 264 (LabMd Email re: Daily IT Rounds); (CX 0236 (LabMd Email re: Daily IT Rounds); (CX 0199 (LabMd Email re: Daily IT Rounds)).

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

236. LabMD hired Hyer as the IT Manager in August, 2009, at which time IT personnel began reporting to Hyer *and* Boyle, with Hyer reporting directly to Boyle as his immediate supervisor. (CX 0704-A (Boyle, Dep. at 12)).

237. Hyer was previously the director of IT at UroCor, and was a mentor to Boyle – both worked together at UroCor in choosing the new billing and laboratory systems for UroCor. (CX 0719, (Hyer Dep. at 17); (CX 0704-A (Boyle Dep. at 110-111)).

238. When Boyle hired Hyer to work for LabMD from June 2009 to March 2012, Hyer signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement on August 24, 2009. (CX 0719 (Hyer, Dep. at 143); (CX 0130 (LabMD Employee Handbook, at 003847)).

239. Upon arrival Hyer found that Curt Kaloustian ("Kaloustian") was not qualified in

any way to meet the demands of his position with LabMD. (CX 0719 (Hyer, Dep. at 41 -42)).

240. LabMd was using TrendMicro or Symantec antivirus software. (CX 0704-A (Boyle, Dep. at 43)).

241. TrendMicro was an overall security system with antivirus protection as one of its functions. LabMD had in place the current version of TrendMicro on its servers and desktops while it was in use during Hyer's tenure. (CX 0719 (Hyer, Dep. at 164 -165)).

242. The system was set up to limit access of physicians to their patients' information only. (CX 0719 (Hyer, Dep. at 142)).

243. TrendMicro created reports and staff reviewed them. (CX 0704-A (Boyle, Dep. at 46)).

244. Antivrus software was used on servers and workstations. (CX 0704-A (Boyle, Dep. at 48)).

245. LabMD had in place firewalls, routers, and Websense to protect its network. (CX 0704-A (Boyle, Dep. at 49)).

246. LabMD established policies regarding employees' passwords and access to information as there were controls by department, by function involving both lab and billing. (CX 0704-A (Boyle, Dep. at 148-149)).

247. In May, 2010, LabMD retained Providyn, Inc. to conduct quarterly scans of LabMD's servers and network which were designed to search for and detect vulnerabilities in applications or in the network that could constitute a security threat. (CX 0704-A (Boyle, Dep. at 34-41); (CX 0044 (Providyn Service Solutions Proposal for LabMD, executed by M. Daugherty)).

248. Under Hyer's direction LabMD addressed and resolved the critical risk items on the Providyn vulnerability scan assessments. (CX 0719 (Hyer, Dep. at 108 -110)).

249. Hyer did not believe that a high priority item on the Providyn vulnerability scan assessment does not equate to a high probability of that risk occurring. (CX 0719 (Hyer, Dep. at 110 -111)).

250. During Hyer's tenure there were no security leaks or data breaches of point to point information being transferred between LabMD and its physician clients – scans of desktops were being run on a daily basis; the security of the servers were tested on a weekly basis. (CX 0719 (Hyer, Dep. at 156 -157)).

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

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

253. LabMD IT employee Christopher Maire ("Maire") started with LabMD in mid-2007 and left in mid-2008. (CX 0724 (Maire, Dep. at 10)).

254. Maire possessed a Bachelor's degree in Information Technology. (CX 0724 (Maire, Dep. at 106)).

255. According to Maire's testimony, during his tenure LabMD had written information security policies, employee handbook, HIPAA compliance and prohibition against personal use of company equipment during his tenure. (CX 0724 (Maire, Dep. at 18-19)).

256. As part of his employment Maire routinely performed daily IT rounds to check on status of all computer systems. (RX 174 – RX 264 (LabMd Email re: Daily IT Rounds); (CX 0236 (LabMd Email re: Daily IT Rounds); (CX 0199 (LabMd Email re: Daily IT Rounds); (CX 0724 (Maire, Dep. at 59)).

257. During Maire's tenure LabMD also had written policies on, audit security operations, internet connectivity policy, monitor security software settings, and operating systems updates. (CX 0006 (LabMD Policy Manual, at 8, 10, 13); (CX 0724 (Maire, Dep. at 21-23)).

258. LabMD had a firewall intrusion-prevention system in place for the period 2007-2008. (CX 0724 (Maire, Dep. at 91)).

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

260. During the period 2007-2008, LabMD had Windows antivirus software installed on its computer system. (CX 0724 (Maire, Dep. at 97)).

261. Maire was not aware of any breach or occurrence of access to information by individuals not authorized to access such information. (CX 0724 (Maire, Dep. at 63-64)).

262. LabMD provided all necessary compliance training regarding the “rules, laws and guidelines regulating its business,” including, but not limited to, HIPAA and HITECH for the period January 2003 to August 2013. (CX 0005 (LabMD Compliance Program, at 1, 2-10); (CX 0127 (LabMD Compliance Training, at 1-28)).

263. Lou Carmichael (“Carmichael”), Compliance Program Manager for LabMD, created the LabMd Compliance Manual and Compliance Training in use for the relevant time period. (CX 0005 (LabMD Compliance Program, at 1–10); (CX 0127 (LabMD Compliance Training, at 1-28); (CX 0708 (Carmichael, Dep. at 26-33)).

264. HIPAA’s Security Rule, Privacy Rule, and extant protections for PHI were part of LabMD’s Compliance Program and Compliance Training for the relevant time period in this case. (CX 0708 (Carmichael, Dep. at 45-46)).

265. LabMD’s Compliance Programs “included regular training on topics including HIPAA, Privacy and Security Regulations.” (CX 0708 (Carmichael, Dep. at 54)).

266. LabMD ran virus scans on its systems. For example, during the period June 2010-July 2010, LabMD ran full virus scans daily on the following systems and/or servers: mapper server; demographics server; LabNet; specialty; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart); (RX 267 (LabMD Server Room Security Chart)).

267. LabMD ran manual scans and ensured RealTime Scanning was active on its systems. For example, during the period June 2010-July 2010, RealTime scanning was active on all LabMD computer systems and/or machines and additional manual scans were initiated as needed. (RX 266 (LabMD Server Room Security Chart); (RX 267 (LabMD Server Room Security Chart)).

268. On June 11, 2010, LabMD utilized Regular Cleaner, TrendMicro, and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart)).

269. On June 11, 2010, LabMD utilized Regular Cleaner, TrendMicro, and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; specialty; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 266 (LabMD Server Room Security Chart)).

270. LabMD used Malwarebytes software on its systems. For example, on the following dates, LabMD utilized Malwarebytes software on the designated systems and/or servers: Mapper Server (June 2& 11, 2010); Demographics Server (June 10-11 & 19, 2010); LabNet (June 4 & 11, 2010); Specialty, HL7/LabCorp, and Automate (June 11, 2010); Supply Orders/Sales Reports (June 1 & 11, 2010); Lytec (June 11, 2010); Visnetic–Email (June 1, 11-12, 14, & 23, 2010). (RX 266 (LabMD Server Room Security Chart)).

271. LabMD used Regular Cleaner and Security Check software on its systems– for example, on July 5, 2010, LabMD utilized Regular Cleaner and Security Check software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Lytec; Visnetic-Email. (RX 267 (LabMD Server Room Security Chart)).

272. LabMD used TrendMicro on its systems – for example, on July 22, 2010, LabMD utilized TrendMicro software on the following systems and/or servers: mapper server; demographics server; LabNet; speciality; HL7/LabCorp; Automate; Supply Orders/Sales Reports; Visnetic–Email. (RX 267 (LabMD Server Room Security Chart)).

273. LabMD used Malwarebytes software on its systems – for example, on thefollowing dates, LabMD utilized Malwarebytes software on the designated systems and/or servers: Mapper Server (July 5, 7, 22, 26 & 29, 2010); Demographics Server (July 1, 5, 14 & 22, 2010); LabNet, Specialty, HL7/LabCorp, Automate, and Supply Orders/Sales Reports (July 5 & 22, 2010); Lytec (July 5, 2010); Visnetic-Email (July 5, 22 & 31, 2010). (RX 267 (LabMD Server Room Security Chart)).

E. **Fisk Testimony**.

274. LabMD's data security expert Adam Fisk ("Fisk") defines the Relevant Time as January 2005 through July 2010. (RX 533 (Fisk, Rep. at 3)).

275. Fisk has "13 years of professional experience building peer-to-peer applications with a focus on computer networking and security." (RX 533 (Fisk, Rep. at 4)).

276. Fisk received his "BA degree in Computer Science and US History from Brown University." (RX 533 (Fisk, Rep. at 4)).

277. "After graduating from Brown, [Fisk] moved to New York, NY to join LimeWire LLC in June of 2000 several weeks after its creation." (RX 533 (Fisk, Rep. at 4)).

278. Fisk is "the former Lead Engineer at LimeWire LLC, the creators of the LimeWire file sharing application, and an expert in peer-to-peer software, computer networking, and data security." (RX 533 (Fisk, Rep. at 3)).

279. Fisk testified LabMD took reasonable steps to secure PHI. (RX 533 (Fisk, Rep. at 32)).

280. LabMD's network adhered to best practices, not merely reasonable ones: It had

two layers of properly configured firewalls protecting the network; there were proper user profiles on employee computers limiting the ability of non-managers to download files from the internet and to install applications. (RX 533 (Fisk, Rep. at 33)).

281. The Cisco 1841 Integrated Services Router deployed at LabMD had both firewall and intrusion prevention capabilities and exceeded the FTC's best practices recommendation. (RX 533 (Fisk, Rep. at 20, 33)).

282. The ZyWall5 IPSec firewall was a redundant layer of protection that shielded the LabMD network from unauthorized intrusion. (RX 533 (Fisk, Rep. at 33)).

283. LabMD did not deploy File Integrity Monitoring; however, LabMD had a policy against employees installing applications not necessary for the performance of their jobs and performed regular checks on employee machines in an effort to ensure that employees adhered to that policy. (RX 533 (Fisk, Rep. at 33)).

284. The best practices guidelines during the Relevant Period did not include File Integrity Monitoring in their recommendations. (RX 533 (Fisk, Rep. at 33)).

285. The 1718 File was not downloaded from LabMD through the firewall or due to any misconfiguration of LabMD's firewall. (RX 533 (Fisk, Rep. at 33)).

286. LabMD's firewall was properly configured and performed just as it should have by blocking incoming connections. (RX 533 (Fisk, Rep. at 33)).

286. Computers running LimeWire do not receive connection requests through the firewall because they are making outgoing connection requests to the Gnutella network. (RX 533 (Fisk, Rep. at 27)).

287. Due to a limited understanding of how LimeWire works, Dr. Hill erroneously

concluded that LimeWire was running as an application accepting incoming connection requests through the firewall. (RX 533 (Fisk, Rep. at 26-27); (CX 0740 (Hill, Rep. at 43)).

288. Consequently, relying solely on the testimony of Kaloustian, Dr. Hill erroneously concluded that the 1718 File was accessed because LabMD's firewall was either disabled or misconfigured. (CX 0740 (Hill, Rep. at 36, 45)).

F. The "Day Sheets."

289. The Day Sheets were found while a search warrant was being served in Sacramento, California on October 5, 2012. (CX 0720 (Jestes, Dep. at 17-24)).

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

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

292. Commission Staff was informed about the Day Sheets one week after the October 5, 2012 raid on the house in Sacramento. (CX 0720 (Jestes, Dep. at 61)).

293. The documents were transmitted to Commission staff in December 2012. (CX 0720 (Jestes, Dep. at 61-62)).

294. The Sacramento Police contacted FTC rather than LabMD because a Google search revealed the investigation arising from FTC's relationship with Tiversa and the 1718 File. (CX 0720 (Jestes, Dep. at 56)).

295. Complaint Counsel has not proven that any of the persons named on the Day Sheets were victims of identity theft. (CX 0720 (Jestes, Dep. at 57)).

296. LabMD was aware of its obligations under HIPAA to notify the patients listed on

the Day Sheets and sent a letter notifying those individuals. (Daugherty, Tr. 1020-1021); (RX 348 (LabMD Patient Notification Letter [redacted])).

297. Hill concluded that LabMD's physical security was adequate. (Hill, Tr. 293).

G. LabMD Is Regulated Under HIPAA/HITECH.

298. At all times relevant, LabMD's PHI data-security practices were regulated by the U.S. Department of Health and Human Services ('HHS') under the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'), 45 U.S.C. § 1320d *et seq*. (U.S. Dep't of Health & Human Servs. (Health Information Technology), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/ (last accessed Aug. 9, 2015); (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5-7 ¶¶ 16-20, 31, 42-43, 48, 72)).

299. Neither HHS nor FTC has accused LabMD of violating HIPAA or HITECH. (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 5-7 ¶¶ 16-20, 31, 42-43, 48, 72)).

300. "The FTC's Complaint in [this] Enforcement Action makes clear that LabMD was a 'health care provider' and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 12 ¶ 42)).

301. "The FTC [has not alleged or proved] that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 13 ¶43)).

302. 123. "The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security." (CX 0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 14 ¶ 48)).

303. "***In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.***" (CX0679 (*LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 15 ¶ 52)) (emphasis added).

H. <u>The Commission Lacks Standards For Medical Companies</u>.

304. Daniel Kaufman, FTC's Rule 3.33 designee and Deputy Direct of the Bureau of Consmuer Protection, was ordered to testify regarding the following topics:

- The 1718 file, including the BOCP's relationship with Tiversa, Dartmouth College, and Eric Johnson.
- All data-security standards that have been used by the BOCP to enforce the law under Section 5 of the Federal Trade Commission Act since 2005.
- Consumers that have been harmed by LabMD's allegedly inadequate security practices.
- Relationship with the Sacramento Police Department relating to documents it found at a Sacramento "flop house" belonging to LabMD.

(Respondent's Deposition Notice of the Bureau of Consumer Protection, *In the Matter of LabMD, Inc., a corporation*, FTC No. 9357 (Jan. 30, 2014) (on file with FTC Complaint Counsel and LabMD Counsel); (Letter from Complaint Counsel Laura Riposo Van Druff, FTC Complaint Counsel, to William A. Sherman, II, LabMD Counsel, regarding Daniel Kaufman's

Rule 3.33 testimony) (Mar. 26, 2014) (on file with FTC Complaint Counsel and LabMD Counsel)).

305. As of the date of the taking of Kaufman's deposition the Commission had not produced information specifically focused on HIPAA Covered Entities, including LabMD, that advised them what was expected, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 176-177)).

306. As of the date of the taking of Kaufman's deposition, the Commission had not conducted any outreach specifically focused on HIPAA Covered Entities to advise them what the Commission expected from them, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 217)).

307. As of the date of the taking of Kaufman's deposition, the Commission had not promulgated any regulations or issued any formal guidance that would inform the general business public what it expected from such Covered Entities, over and above HIPAA, to comply with Section 5. (RX 525 (Kaufman, Dep. at 215)).

308. Kaufman testified that the general business public must visit the FTC web site, review the FTC's complaints, orders, business education materials, attend FTC seminars and speeches, follow the FTC blog, follow FTC testimony before Congress, review FTC settlements, review FTC complaints, review FTC orders, review FTC press releases about data security cases, look at SANS, NIST and look at software and hardware product literature to determine what Section 5 requires in each given case. (RX 525 (Kaufman, Dep. at 190; 207-210); (Initial Pretrial Conference, *In the Matter of LabMD, Inc., a* corporation, FTC No. 9357, at 9-10) (Sept. 25, 2013)) (JUDGE CHAPPELL: "Have you -- in that regard, has the Commission issued guidelines for companies to utilize to protect this information or is there something out there for

a company to look to?" MR. SHEER: "There is nothing out there for a company to look to. … JUDGE CHAPPELL: "Is there a rulemaking going on at this time or are there rules that have been issued in this area?" MR. SHEER: "There are no -- there is no rulemaking, and no rules have been issued …"); (RX 532 (Kaufman, Dep. at 163-220).

309. The thousands of pages of materials Complaint Counsel produced to LabMD in response to a request for information regarding standards consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief) (N.D. Ga.), at 16-17 ¶ 57)).

310. Some of these materials are of very recent vintage and dated after the events described in FTC's August 2013 administrative complaint allegedly occurred. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief) (N.D. Ga.), at 16-17 ¶ 57)).

311. Some of these materials are dated after August 28, 2013, when FTC issued this complaint. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 16-17 ¶ 57)).

312. The only regulations that FTC enforcement staff produced to LabMD did not

apply to LabMD and implemented statutes that also did not apply to LabMD. (CX 0679 (*LabMD v. FTC* (Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), at 16-17 ¶ 57)).

I. <u>Dr. Hill</u>.

313. In May, 2013, the Commission contacted Dr. Hill and asked her to assess LabMD's security program. She agreed to provide services to the FTC at that time. (RX 524 (Hill, Dep. at 55-56)).

314. Dr. Hill admits that portions of her report follow closely along with the allegations contained in paragraph 10 of the Complaint. (RX 524 (Hill, Dep. at 58)).

315. Hill relied upon the following materials in formulating an opinion in her report: (1) transcripts and exhibits from the FTC's investigational hearings and depositions of LabMD, its current and former employees, and third parties; (2) documents and correspondence provided to Complaint Counsel by LabMD and third parties in connection with the FTC's pre-Complaint investigation or this litigation; (3) industry and government standards, guidelines, and vulnerability databases that establish best practices for information security practitioners. (RX 524 (Hill, Dep. at 59-60)).

316. Hill states that Google is the place where an individual without her education, background, and experience could go to determine the industry and government standards and guidelines, as well as vulnerability databases, which establish best practices for the information security practitioner. (RX 524 (Hill, Dep. at 91-92)).

317. Other than the HIPAA Security Rule, Hill did not review any other portions of HIPAA in formulating her expert opinion. (RX 524 (Hill, Dep. at 65-66)).

318. Dr. Hill did not (a) testify to knowledge of HIPAA data security regulations; (b) compare LabMD's PHI data security acts and practices with that of other healthcare providers of LabMD's size and nature; (c) consider LabMD's size notwithstanding HIPAA's emphasis on scalability. (Hill, Tr. at 296) ("For both—for small organizations and for large organizations, the guidelines are consistent"); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007); U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. Pts. 160, 162, & 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015); did not consult any medical industry data-security practices; did not apply the Commission's "reasonable" test but rather a more stringent "best practices" test; (d) identify best practices for each of the years during the relevant time (2005-2010), instead using 2014 standards and looking back (RX533 (Fisk, Rep. at 31-32); (e) profess knowledge of or apply medical industry standards; or (f) *"consider the FTC standards and guidelines"* in formulating her opinion whether LabMD's data security was reasonable.). (Hill, Tr. 230-231, 240-241) (emphasis added)).

319. Dr. Hill testified that "there's no such thing as perfect security, especially whenever there are humans involved in the configuration of the software." (Hill, Tr. 100).

320. At her deposition on April 18, 2014, Hill testified she referred exclusively to the HIPAA Security Rule in her report. (RX524 (Hill, Dep. at 64-65)).

321. At trial, Hill testified that she considered both the HIPAA Security Rule and HIPAA's six basic rules for assessment. (Hill, Tr. 231-232).

322. Dr. Hill does not know whether HIPAA "governs the storage and transfer of health-related information by medical care providers." (Hill, Tr. 231).

323. Hill did not consider the HIPAA Security Rule or HIPAA in deciding whether or not LabMD was a HIPAA-covered entity. (Hill, Tr. 231) (Q. "So you're not intimately familiar with HIPAA then." A. "No, sir." Q. "Okay. And you did not consider HIPAA or HIPAA's guidelines in the formulation of your opinion in this case; correct?" A. "I considered the HIPAA security rule portion." Q. "And that's all with regard to HIPAA?" A. "Yes." Q. "And so it didn't play into your consideration or your opinion as to whether or not LabMD was a HIPAA-covered entity." A. "No. I didn't take that into consideration.").

324. Hill agrees LabMD received, maintained, utilized and stored health information. (RX 524 (Hill, Dep. at 65)).

325. Hill was not instructed by the FTC to give an opinion regarding HIPAA in the case against LabMD. (RX 524 (Hill, Dep. at 66)).

326. Hill admits that LabMD's physical data security was adequate. (RX 524 (Hill, Dep. at 118-119)).

327. Dr. Hill's report states: "For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information." (Hill, Tr. 216-219); (CX 0740 (Hill, Rep. at 20 ¶ 49)).

328. Dr. Hill was not asked by the FTC to assume that the type of harm set forth at page 20, ¶ 49 of her report actually had occurred. (Hill, Tr. 217); (CX 0740 (Hill, Rep. at 20 ¶49)).

329. Dr. Hill has no opinion with regard to the likelihood of harm because it was assumed in her report. (Hill, Tr. 218); (CX 0740 (Hill, Rep. at 20 ¶49)).

330. Dr. Hill relies on CX0019 and the claim of Robert Boback and Tiversa that the 1718 File was found in four (4) places. (CX 0740 (Hill, Rep. at 17 ¶ 46)) ("A list of the materials that I considered in reaching my opinions is attached to this report as Appendix B."); (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found)); (CX 0740 (Hill, Rep. at 19, 59, 61)).

331. Dr. Hill did not consider HIPAA's definition of protected health information in formulating her opinion about LabMD data security practices. (RX 524 (Hill, Dep. at 71)).

332. Hill did not consider the fact that LabMD was a covered entity as defined by HIPAA. (RX 524 (Hill, Dep. at 71)).

333. Hill did not rely on the data security standards published by the FTC. (Hill, Tr. 230-231); (RX 524 (Hill, Dep. at 71-72)).

334. HIPAA is based on risk assessment and scalability, which Hill's reports and opinions fail to properly consider. (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3 ("Factors that determine what is 'reasonable' and 'appropriate' ***include cost, size, technical infrastructure and resources.***") (emphasis added), 12 ("***The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances.*** Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L.

No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)).

332. "The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity." (HHS: The Security Rule, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html) (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)).

333. "The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information." (HHS: The Security Rule, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html) (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007)); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007)).

333. HHS does not require what Dr. Hill does with respect to data encryption and integrity monitoring and are more prescriptive than HIPAA or inconsistent with HHS guidance, including encryption at rest (an addressable requirement of 45 C.F.R. § 164.312(a)(1)), encryption in transit (an addressable requirement of 45 C.F.R. § 164.312(e)(1)), and file integrity monitoring (not addressed specifically by the Security Rule). (CX 0740 (Hill, Rep. at

20 ¶ 55, 22-23 ¶ 61(b)(bullet 2), 24-25 ¶ 65, 26-28 ¶ 68(c), ¶ 69)); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007), 12)) ("***Covered entities use open networks such as the Internet and e-mail systems differently*.** ***Currently no single interoperable encryption solution for communicating over open networks exists*. *Adopting a single industry-wide encryption standard in the Security Rule would likely have placed too high a financial and technical burden on many covered entities. The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use. A covered entity should discuss reasonable and appropriate security measures for the encryption of EPHI during transmission over electronic communications networks with its IT professionals, vendors, business associates, and trading partners.***") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last accessed Aug. 9, 2015); (Dep't of Health & Human Servs. (HIPAA Security Series (**4 Security Standards: Technical Safeguards**) (Volume 2/ Paper 4) (5/2005: rev. 3/2007), at 15-17) (Security Standards Matrix (Appendix A of the Security Rule)), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (last accessed Aug. 9, 2015)).

334. Dr. Hill's opinion on risk assessment based upon NIST Security Series Reference 800-30 conflicts with HIPAA guidance and regulations. (CX 0740 (Hill, Rep. at 29-30 ¶ 74); (Dep't of Health & Human Servs. (HIPAA Security Series (**6 Basics of Risk Analysis and Risk Management**) (Volume 2/ Paper 6) (6/2005: rev. 3/2007), 3)) ("…**only federal agencies are required to follow federal guidelines like the NIST 800 series** … ***Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that***

organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.") (italic emphasis in original) (bold emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf (last accessed Aug. 9, 2015).

335. Dr. Hill has never given an opinion regarding the adequacy of a company's operating on a day-to-day basis and has no medical industry experience. (RX 524 (Hill, Dep. at 73)).

336. In rendering her opinion, Dr. Hill has never conducted an on-site visit to a business to review its existing data security as it operates on a day-to-day basis. (RX 524 (Hill, Dep. at 73)).

337. In rendering her opinion, Dr. Hill has never conducted an on-site visit to a business (including LabMD, in this case) to review and evaluate its existing data security polices, practices, and procedures. (RX 524 (Hill, Dep. at 73)).

338. Dr. Hill formulated the definition of "comprehensive information security program" in her report based solely on her personal experience. (RX 524 (Hill, Dep. at 73-74) (Ex. 1 at p. 19 ¶ 52) (as Dep. Ex. RX-1)).

339. The primary information Dr. Hill used for reaching the conclusions in her report regarding LabMD's data security was her background and experience. (RX 524 (Hill, Dep. at 86)).

340. Hill did not rely on FTC's "five key principles" to data security listed in the "Protecting Personal Information: A Guide for Business" issued November 2011 – the "five key

principles" do not match Dr. Hills "seven factor test" and do not include "defense in depth," which Dr. Hill testified LabMD was supposed to have discovered in 2009. (Hill, Tr. 235-236); (Fed. Trade Comm'n, Protecting Personal Information: A Guide to Business (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf (last accessed Aug. 9, 2015)).

341. The Commission has never published data security standards or guidance for medical service providers regulated by HIPAA or, prior to this case, suggested Section 5 might prohibit what HIPAA permits. (RX 526 (Complaint Counsel's Amended Response to LabMD's Requests For Admission No. 1, at 4 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9257) (Apr. 1, 2014)).

342. Between 2005 and 2010, the FTC did not prescribe any rules or promulgated regulations regarding data-security, data security practices or data security standards for PHI that defines what acts are prohibited or required under Section 5 of the FTC Act, 15 U.S.C. § 45, as related to PHI. (RX 526 (Complaint Counsel's Amended Response to LabMD's Requests For Admission No. 1, at 4-5 (In the Matter of LabMD, Inc., a corporation, FTC No. 9257) (Apr. 1, 2014)).

343. FTC's Deputy Director of BCP and designated Rule 3.33 witness, Daniel Kaufman admitted that the FTC lacks any Section 5 "unfairness" data security standards and that the FTC has not promulgated data security regulations. (RX525 (Kaufman, Dep. at 211, 215)) (Q. "So does the term "data security" appear in Section 5 of the Act?" A. "No, it does not.") (Q. "It's correct that the FTC has not promulgated regulations with regard to data security for personal identifying information?" A. "In connection with Section 5 of the FTC Act, that is correct. We have, nevertheless, consistently applied Section 5 and the unfairness test to assess

the reasonableness of the security practices." Q. "But that's not promulgation of regulation; is that correct?" A. "Yes.").

344. Dr. Hill's testimony is inconsistent in stating that she "was not asked to make any assumptions about the inadequacies of LabMD's data security" while also assuming that the 1718 File was taken from LabMD's possession as a result of inadequate data security. (Hill, Tr. 219-220) (Q. "Were you asked to assume that the 1718 File escaped the possession of LabMD due to some inadequacy in LabMD's data security?" A. "I was not asked to make any assumptions about the inadequacies of LabMD's data security.").

345. Dr. Hill states "[t]here's no definitive evidence of how [the 1718 File] left LabMD's possession" as a result of the downloading of an unauthorized program onto a workstation at LabMD. (Hill, Tr. 220).

346. Dr. Hill did not have access to the Wallace testimony. (Wallace, Tr. 1337); (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Tr. 80-325) (Hill testimony) (May 20, 2014)).

347. Dr. Hill has no opinion about exactly how the 1718 File was taken from LabMD. (Hill, Tr. 219).

348. Dr. Hill failed to address scalability as required by HIPAA. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. Pts. 160, 162, & 164) (2007); (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3, ("***Factors that***

determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources.") (emphasis added), 12 ("***The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts.***") (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164)).

349. The 1996 HIPAA statute states that in promulgating information security regulations, the Secretary must take into account the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary), and the preamble to the HIPAA Security Rule (p. 8335) states accordingly that one of the foundations of the rule is that it should be scalable, so that it can be effectively implemented by covered entities of all types and sizes. (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

350. Based upon public comments received during the rulemaking process for HIPAA's Security Rule, HHS crafted a unique information security regulatory scheme that separated 'implementation specifications – the types of very specific security requirements emphasized by the FTC's expert – into two classes: "required" and "addressable." (60 Fed. Reg. 8336 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

351. HHS stayed consistent with the original information security regulatory separated, “two–class” theme in its most recent updates to the HIPAA Privacy and Security rules in 2013. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162,164); (U.S. Dep’t of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last visited Aug. 9, 2015)).

352. HHS utilized a scalable model in promulgating HIPAA’s Privacy and Security Rules, such that these Rules reflect HHS’s challenge in complying with Congressional intent in establishing a security rule to address reasonable and appropriate security requirements for the range of organizations in healthcare that differ greatly in operations, size, complexity, and resources. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162,164); (U.S. Dep’t of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last visited Aug. 9, 2015)).

353. HIPAA demands that a covered entity perform a risk assessment in good faith and take actions to secure Electronic Protected Health Information (“EPHI”) based on the findings of that risk assessment. (74 Fed. Reg. 42740, 42760 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 164, §164.402(2)(i-iv); (U.S. Dep’t of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, at 71, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013)), *available at*

http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015)).

354. In assessing HIPAA noncompliance, it is necessary to determine if a risk assessment was performed in good faith, and resulted in a process that included implementation of requirements and appropriate responses to "addressable" issues. (74 Fed. Reg. 42740, 42760 (Aug. 24, 2009) (codified at 45 C.F.R. pts. 164, §164.402(2)(i-iv); (U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text, at 71, 45 C.F.R. pts. 160, 162, 164 (as amended through Mar. 26, 2013), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf (last accessed Aug. 9, 2015)).

355. Given the limited knowledge of information technology by many small health care providers, especially during the early years of HIPAA Security, many of the security measures they were advised to adopt by HHS issued guidance related to physical and administrative security rather than specific technical security. (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164)).

356. The preamble to HIPAA's Security Rule provides "that encryption should not be a mandatory requirement for transmission over dial-up lines. . . . [and] when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting email communications with patients. . . . [so] the use of encryption in the transmission process [is] an addressable implementation specification." (60 Fed. Reg. 8335, 8357 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164) (corresponding to 45 C.F.R. §164.312(e)(1) of the Rule on Transmission Security)).

357. After almost ten years of complying with HIPAA security rules, the guidance has not changed substantively regarding implementing security for small providers in the healthcare industry, based upon HHS's understanding of the realities associated with implementing security for small providers in the healthcare industry. (U.S. Dep't of Health & Human Servs., Office of the Nat'l Coordinator for Health Info. Tech., Guide to Privacy & Security of Electronic Health Info., 13-14 (Version 2.0) (Apr. 2015), *available at* http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf (last accessed Aug. 9, 2015)).

355. Dr. Hill's opinion did not reference or rely on the relevant HIPAA statutes, regulations and guidance. (RX 524 (Hill. Dep.) (Apr. 18, 2014)); (CX 0740 (Hill Rep.) (Mar. 18, 2014)); (Hill, Tr. 80-325); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)).

356. Dr. Hill did not properly apply the accordance with the HIPAA Security Rule, and did not take account, as required by the 1996 HIPAA statute, the needs and capabilities of small health care providers such as LabMD. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)).

357. Dr. Hill opined that between January 2005 and July 2010 "LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failings at relatively low cost using readily available security measures." (CX 0740 (Hill, Rep. at 20)).

358. Her opinion does not specify precisely how LabMD failed at any given point in

time. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

359. Hill further opined that "LabMD did not develop, implement or maintain a comprehensive information security program to protect consumer's Personal Information." (CX 0740 (Hill, Rep. at 24)).

360. According to Dr. Hill, maintaining a comprehensive information security program includes employing a defense in depth strategy, which in turn includes addressing the seven principles she outlines in her report. (Hill, Tr. 307-309).

361. The seven principles are: (1) Don't keep what you don't need, (2) Patch, (3) Ports, (4) Policies, (5) Protect, (6) Probe, and (7) Physical. (CX 0740 (Hill, Rep. at 13-15)).

362. Dr. Hill is unaware of any document that cites there are "seven principles for a comprehensive information security program." (Hill, Tr. 242-243).

363. Dr. Hill opines on data security standards relating to the general Information Technology industry. (CX 0740 (Hill, Rep. at 1-46); (Hill, Tr. 234); (RX 524 (Hill, Dep. at 61)).

364. Dr. Hill admits that she has never worked for a medical provider or lab. (RX 524 (Hill, Dep. at 150)).

365. Dr. Hill only became aware of the defense in depth strategy circa mid-2009. (Hill, Tr. 306).

366. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that penetration testing was never done. CX 0740 (Hill, Rep. at 38); (Hill Tr. 276)).

367. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that firewalls were disabled on servers that contained personal information. (CX 0740 (Hill, Rep. at 38); (Hill, Tr. 274-275).

368. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that personal information was transmitted and stored in an encrypted format. (CX 0740 (Hill, Rep. at 38)).

369. Dr. Hill relies only on factual information from Kaloustian's Investigational Hearing Transcript to conclude that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft. (CX 0740 (Hill, Rep. at 42)).

370. Dr. Hill relies only on factual information from Curt Kaloustian's Investigational Hearing Transcript to conclude that LabMD had several firewalls, including the firewall that was part of its gateway router and internal firewalls, but these firewalls were not configured to prevent unauthorized traffic from entering the network. (CX 0740 (Hill, Rep. at 47)).

371. Kaloustian was compelled to give testimony pursuant to a FTC Civil Investigative Demand. (CX 0750 (CID to Curt Kaloustian)).

372. The nonpublic proceeding took place on May 3, 2013 before FTC attorneys Laura Riposo Van Druff and Alain Sheer. (CX 0735 (Curt Kaloustian, IHT (with attached Errata), at 1-7)).

373. Prior to this hearing, on March 20, 2013, Commission staff was notified by LabMD's counsel that contacting former employees of LabMD was improper without first informing the company's legal counsel so as to properly preserve the attorney-client privilege and that Kaloustian was subject to a confidentiality agreement. (CX 0735 (Curt Kaloustian, IHT (with attached Errata), at 1-7)).

374. LabMD was never told Kaloustian was to be deposed by FTC. (CX 0735 (Curt Kaloustian, IHT (with attached Errata) at 1-7)).

375. LabMD did not have counsel present and could not assert the attorney-client privilege. (CX 0735 (Curt Kaloustian, IHT (with attached Errata) at 1-310)).

376. At the time he testified to FTC on May 3, 2013, Kaloustian had been terminated by LabMD for inadequate work performance. (RX 415 (Kaloustian background check/A. Simmons' resignation, at 1)) ("Terminated for failure to perform job duties").

377. Dr. Hill only relies on information from Robert Boback and Tiversa to conclude that "[c]opies of the 1718 File were found on computers in California, Arizona, Costa Rica, and the United Kingdom." (CX 0740 (Hill, Rep. at 17)).

378. Dr. Hill admits that in rendering her expert opinion that LabMD's data security was insufficient, that she does not cite to any purported FTC standards and guidelines. (Hill, Tr. 230-23, 240-241).

379. Dr. Hill was not asked and did not opine regarding LabMD's current data security practices or whether those practices now cause substantial consumer injury and are unreasonable. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

380. Dr. Hill was not asked and did not opine whether the allegedly unreasonable LabMD's data security practices during the 2005-2010 time-frame are "likely" or probable to reoccur, and if so, to cause harm in the future. (ALJ Chappell, Tr. 513-514) ("The rule is, a witness who's an expert is limited to opinions contained in the expert report that is vetted properly through discovery. . . ."); (Hill, Tr. 218) ("Q. So it's fair to say then that you have no opinion with regard to the likelihood of harm because it was assumed in your report; correct? A. I have no opinion, yes.").

381. To the extent Dr. Hill did opine regarding the likelihood of harm, that opinion was based on perjured and fraudulent evidence provided by Boback and Tiversa. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

382. Although Dr. Hill considered LabMD's data security for the time period of 2005-2010, she used and evaluated sources published *after* 2010. (CX0740 (Hill, Rep. at 4-8)).

383. Dr. Hill did not consider FTC's standards and guidelines in formulating her opinion. (Hill, Tr. 230-31, 240-41).

384. Complaint Counsel did not ask Dr. Hill to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

385. Complaint Counsel did not ask Dr. Hill to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. (RX 524 (Hill. Dep.) (Apr. 18, 2014); (CX 0740 (Hill Rep.) (Mar. 18, 2014); (Hill, Tr. 80-325)).

J. **Rick Kam**.

386. Complaint Counsel hired Rick Kam to provide an opinion regarding the "risk of injury to consumers caused by the unauthorized disclosure of their sensitive personal information." (CX 0742 (Kam, Rep. at 5)).

387. FTC paid Kam "$350 per hour" for his opinions and testimony against LabMD. (CX 0742 (Kam, Rep. at 5); (LabMD's Mtn. *In Limine* to Exclude Kam's Testimony, at 1 (*In the Matter of LabMD, Inc., a corporation*, FTC Dkt. No. 9357, FTC Doc. No. 264) (Apr. 22, 2014))

[redacted]

[redacted] (RX 522 (Kam, Dep. at 181); Kam is not qualified to testify as an expert on the risk of harm to consumers because he [redacted] (LabMD's Mtn. In Limine to Exclude Kam's Testimony (*In the Matter of LabMD, Inc., a corporation,* FTC No. 9357, at 8 (Apr. 22, 2014); (RX 522 (Kam, Dep. at 181-182)).

388. Kam's only educational degree is in management and marketing. (Kam, Tr. 516).

389. Kam has no expertise in computer data security or computer network security. (Kam, Tr. 518).

390. Kam's personally-developed methodology is not generally accepted in the fields of medical or data privacy or statistical analysis, nor has any work based upon such methodology been peer-reviewed or published. (CX 0742 (Kam, Rep. at 17-18); (RX 522 (Kam, Dep. at 46)).

391. In developing his personal four–factor methodology, Kam never used statistical analysis, never spoke to data privacy professionals, and never allowed any review of his methodology because of confidentiality agreements in place. (Kam, Tr. 549-552) (Q. "All of your work with your clients is subject to confidentiality agreements; right?" A. "Yes." . . . Q. "Well, did you consult statistical analysis to develop your four factors?" A. "I don't believe I used statistical analysis to develop that." . . . Q. "Did you discuss with these other privacy professionals how many factors to include in the test?" A. "You know, I don't recall asking – thinking about it in that context. No.").

392. Kam's personally-developed methodology has never been published, peer reviewed, or reviewed in any form. (Kam, Tr. 552).

393. All of Kam's work has been under the patronage of client-consulting arrangements governed by confidentiality agreements. (RX 522 (Kam, Dep. at 48-49) [redacted] (LabMD's Mtn. *In Limine* to Exclude Kam's Testimony, at 4 (FTC Doc. No. 264) (Apr. 22, 2014)).

394. Kam's methodology, report, and opinions they cannot be tested or publicly reviewed due to governing confidentiality agreements and the fact that such methodology was developed by Kam in consultation with hiring counsel. (Kam, Tr. 551-552); (RX 522 (Kam, Dep. at 46)) (Q. [redacted]

395. Complaint Counsel provided Kam with the "Transcript of the deposition of Robert Boback, CEO of Tiversa, dated November 21, 2013, with supporting exhibits," including CX0019, upon which Kam based his report, opinions, and testimony. (CX 0742 (Kam. Rep. at 6)).

396. Kam is the "president and co-founder of ID Experts . . . based in Portland, Oregon." (CX 0742 (Kam, Rep. at 3)).

397. Lawrence Ponemon sat on the board of advisors for Kam's company for six (6) to nine (9) months in 2013. (RX 522 (Kam, Dep. at 172-174).

398. Kam knows Lawrence Ponemon is on the board of advisors for Tiversa. (Kam, Tr. 552-553).

399. Kam used and relied upon the 2013 Ponemon Survey in his report, opinions, and testimony. (Kam, Tr. 484-486); [redacted]

[redacted]

401. Kam's company ID Experts paid $50,000 to the Ponemon Institute for a 2014 data privacy and security report. (Kam, Tr. 554).

402. Kam agreed with the following conclusion regarding medical identity theft contained in the 2013 Ponemon survey: [redacted]

403. The response rate to the 2013 Ponemon Survey was 1.8 %. (Kam, Tr. 540).

404. Kam did not conduct a regression analysis for the 2013 Ponemon Survey because he is not a statistician and does not know the definition of a regression analysis. (Kam, Tr. 540) (Q. "Mr. Kam, do you know what a regression analysis is?" A. "I'm not a statistician. I wouldn't be able to give you an accurate definition." Q. "So then you didn't conduct a regression analysis on the Ponemon survey, did you?" A. "No.").

405. The 2013 Ponemon Survey had a non-response bias. (Kam, Tr. 540) (Q. "Do you know what a nonresponse bias is?" A. "I believe so." Q. "What is it?" A. "It's if people who

were not -- who were surveyed did not respond might have a different answer to the question." Q. "Under your understanding of a nonresponse bias, the Ponemon survey has a nonresponse bias, doesn't it?" A. "Yes, it does.").

406. The 2013 Ponemon Survey is unreliable because it collected results using a Web-based collection method, and compensated respondents. (Kam, Tr. 541) (Q. "The Ponemon survey collected its results using a Web-based collection method, didn't it?" A. "I believe that to be the case. Yes." Q. "The Ponemon survey compensated respondents, didn't it?" A. "They did, yes.").

407. The 2013 Ponemon Survey has a sampling frame bias. (Kam, Tr. 541) (Q. "Do you know what a sampling frame bias is?" A. "I believe it has something to do with the sample and who was actually -- who actually took the survey." Q. "The Ponemon survey has a sampling frame bias, doesn't it?" A. "It does. . . .").

408. Kam relied upon Robert Boback's November 2013 testimony when analyzing the risk of harm under the first three (3) factors of his four-factor test. (Kam, Tr. 542).

409. Kam assumed as true Robert Boback's November 2013 testimony that law enforcement had apprehended someone suspected of identity theft or fraud using one of the addresses where the 1718 File was found. (Kam, Tr. 542).

410. Kam relied upon Robert Boback's November 2013 testimony and multiple levels of hearsay and supposition regarding IP address 173.16.83.112. (Kam, Tr. 544-545) (Q. "On page 64 line 17, Mr. Boback says, of one of the IP addresses, 'I believe that the 173.16.83.112 had law enforcement, federal law enforcement after that individual for identity theft or fraud of some sort. Tiversa wasn't involved in that, though. QUESTION: 'How do you know this?' ANSWER: 'We heard this through federal law enforcement, you know, surreptitiously through

federal law enforcement. But we don't know specifically.' Did I read that correctly?" A. "Yes." Q. "Mr. Boback says 'I believe' instead of 'I know.' . . ." Q. "Mr. Boback says 'I believe' instead of 'I know,' doesn't he?" A. "He does say that in his testimony." Q. "He uses the word 'surreptitiously'?" A. "Yes." Q. "He says he doesn't know specifically about the incident." A. "I agree.").

411. Kam used unreliable, double hearsay evidence found at pages 64-65 of Robert Boback's November 2013 deposition as the factual underpinning for Kam's assessment of the risk of harm in this case. (Kam, Tr. 545-546) (Q. "When asked, on page 64, 'Do you know what action was taken?' Mr. Boback answered, on page 65, 'I had heard that the individual at 173.16.83.112 was either detained or arrested in an Arizona Best Buy buying multiple computers. I don't know the outcome of this case. I'm not privileged to any of that information.' Did I read that correctly?" A. "You did." Q. "Mr. Boback says he heard the individual was detained or arrested instead of he knew; isn't that right?" A. "Yes." Q. "He doesn't say who he heard it from?" A. "No." Q. "He does not say who was arrested?" A. "No. . . ." Q. "He says he doesn't know the outcome of the case pertaining to identity theft in Arizona; right?" A. "Yes." Q. "And you used this information as the factual underpinning for your assessment of the risk of harm; right?" A. "For some of it, yes.").

412. Kam relied upon the CLEAR spreadsheet. (CX 0742 (Kam, Rep. at 7, 23); (Tr. 371-373)).

413. The CLEAR spreadsheet was excluded from evidence. (ALJ Chappell, Tr. 371-373)) (JUDGE CHAPPELL: ". . . to the extent you want to use this document against respondents, and if I understood what you said, to show that these Social Security numbers were used and that might for some later witness be used to say that's indicative of a possible identity

theft, ***we don't know if the Social Security number on the day sheet was correct.*** We don't know if the Social Security number that the CLEAR data reflected was accurate. . . .") (emphasis added)).

414. Kam cannot identify a single actual victim of identity theft caused by LabMD's acts or practices. (Kam, Tr. 507).

415. For the relevant time period 2007-2010, Kam cannot identify a single actual victim of identity theft or fraud among the names on the LabMD Day Sheets. (Kam, Tr. 507) (Q. ". . . [D]o you know of any actual victims of identity theft or fraud . . . among the names that were on the LabMD day sheets in 2007?" A. "No." Q. "In 2008?" A. "No." Q. "In 2009?" A. "No." Q. "In 2010?" A. "No.").

416. Complaint Counsel instructed Kam to assume LabMD's data security practices were unreasonable for the Relevant Time. (Kam, Tr. 517-518) (Q. "At the bottom of page 5, you wrote, 'For the purposes of my analysis, I have assumed that LabMD failed to provide reasonable and appropriate security for consumers' personal information maintained on its computer networks.' Did I read that correctly?" A. "You did." Q. "So in your expert opinion, in providing your expert opinion, you're not analyzing any of LabMD's specific practices with respect to its computer networks; correct?" A. "Correct.); (Kam, Tr. 518) (Q. "You don't know the degree to which LabMD's data security practices were adequate or not, you just assumed they were inadequate; correct?" A. "That's correct.").

417. Kam testified at trial that his report would be "valid in full" even if LabMD had "executed exemplary levels of data security practices" at all times relevant to this case. (Kam, Tr. 521) (Q. "So, Mr. Kam, your testimony is that even if it were found that LabMD had

executed exemplary levels of data security practices, your report would still be valid in full." A. "Given what I just said earlier, yes.").

418. Kam relied on Robert Boback's testimony to conclude that the 1718 File was found on four IP addresses, and was available as late as November 21, 2013 on the peer to peer network. (CX 0741 (Van Dyke, Rep. at 7)).

419. Kam assumed that the suspects in whose Sacramento house LabMD's Day Sheets were found had "identity theft charges and convictions prior to the events in Sacramento on October 5, 2012." (RX 522 (Kam, Dep. 147-148)).

420. Kam estimated that there would be 76 victims of medical identity theft due to the alleged disclosure of the 1718 File. (CX 0742 (Kam, Rep. at 19)).

421. Kam admitted that his expert opinion did not account for the absence of any evidence of victims in this case. (Kam, Tr. 532).

422. Kam repeatedly mentions the possibility of embarrassment, specifically from the alleged exposure of CPT codes, which indicate that a person has paid for a particular laboratory test to be run, as an element of damage. (CX 0742 (Kam, Rep. at 16, 21)).

423. Kam acknowledges that CPT codes indicate only that testing has been paid for, and do not "indicate a diagnosis." (CX 0742 (Kam, Rep. at 16)).

424. Complaint Counsel did not ask Kam to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. (CX 0742 (Kam Rep.); (RX 522 (Kam Dep.); (Kam, Tr. 377-573)).

425. Complaint Counsel did not ask Kam to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. Kam's testimony suggest bias as his

method was simply to place the heaviest weight on whichever factor disfavored LabMD most. (CX 0742 (Kam Rep.); (RX 522 (Kam Dep.); (Kam, Tr. 377-573)).

426. Kam admitted that in *every* data breach in his professional experience a victim has come forward with an injury. (Kam, Tr. 532).

427. Kam admitted that his expert opinion did not account for the absence of any evidence of victims in this case. (Kam, Tr. 532).

K. <u>Jim Van Dyke.</u>

428. Jim Van Dyke ("Van Dyke") was engaged by FTC to "assess the risk of injury to consumers whose personally identifiable information has been disclosed by LabMD, Inc. without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure." (CX 0741 (Van Dyke, Rep. at 2)).

429. Complaint Counsel did not ask Van Dyke to opine whether LabMD's post-July, 2010 data security practices were unreasonable or inadequate. [redacted]

430. Complaint Counsel did not ask Van Dyke to opine whether the allegedly unreasonable and inadequate LabMD's data security practices during the Relevant Time are "likely," probable, or even possible to reoccur and to cause harm in the future. [redacted]

431. Van Dyke assumed that "LabMD failed to provide reasonable and appropriate for the personally identifiable information maintained on its computer networks." (CX 0741 (Van Dyke, Rep. at 2)).

432. Van Dyke also assumed that the "1718 File and the day sheets were found outside of LabMD as a result of a data breach." (Van Dyke, Tr. 678-679).

433. Van Dyke's opinion was "LabMD's failure to provide reasonable and appropriate security for [the 1718 File, Day Sheets, and personally identifiable information maintained on LabMD's computer network] places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of what is commonly called "identity theft . . ." (CX 0741 (Van Dyke, Rep. at 3)).

434. Van Dyke's opinions were based on pre-January 2010 practices only. (CX 0741 (Van Dyke, Rep. at 2, 4)).

435. Van Dyke admitted that he does not have extensive educational experience with information technology. (RX 523 (Van Dyke, Dep. at 11-13, 19)).

436. Van Dyke is not a statistician. (Van Dyke, Tr. 674) (Q. "[Mr. Van Dyke,] you're not a statistician; correct?" A. I'm not personally a statistician, no."); (Van Dyke, Tr. 718-719)) (JUDGE CHAPPELL: "And you, if I take it -- if I'm correct, do not have a statistical background; is that correct?" THE WITNESS: "I think it's most accurate to say I do have a statistical background. I do not have a dedicated educational degree in statistics, no, but I've worked in that field and taken dedicated courses in that subject." JUDGE CHAPPELL: "Would you call yourself a statistician?" THE WITNESS: "No, I would not, Your Honor.").

437. Complaint Counsel first contacted Van Dyke to serve as an expert in this case before the Knowledge Networks Survey was fielded in October 2013. (Van Dyke, Tr. 636) (Q. "And the survey was fielded by Knowledge Networks in October of 2013?" A. "Correct." Q. "Do you know how long from the time the survey was first fielded or sent to the panel that the survey was completed?" A. "To the best of my recollection, that fielding began on October 9, 2013 and concluded on October 23, 2013. . . ."); (Van Dyke, Tr. 638) (Q. ". . . When were you contacted by the FTC to – when did they ask if you would be willing to render an opinion in this

case?" A. "Oh, I could not answer with precision on that. That was sometime in the first half of 2013." Q. "Okay. So it was prior to the survey being fielded; correct?" A. "That is correct.")).

438. Van Dyke admits that he never considered any of the specific facts of the case. (RX 523 (Van Dyke, Dep. at 72-73) (Q. "So your entire opinion is based on the responses to the survey that was conducted in October of 2013?" A. "Yes, for the purpose of this statement that's true, yes." Q. "So the actual facts of the LabMD case, outside of the presumption that the information was exposed to unauthorized third parties, really doesn't matter and really wasn't taken into consideration in your analysis when it comes to these percentages; correct?" A. "That's correct." Q. "And the actual facts of what actually happened in the case concerning LabMD do not play a factor in your conclusions and opinions as it relates to how much time a consumer will spend correcting what occurred as a result of the LabMD breach; correct?
A. ". . . THE WITNESS: Yes, that is correct, yes.")).

439. Van Dyke did not contact any of the referring physicians' patients listed in the 1718 File. (CX 0741 (Van Dyke, Rep. at 1-21)).

440. Van Dyke's report and opinions rely on Boback's November 2013 testimony. (RX 523 (Van Dyke, Dep. at 107-108) (Q. . . . "You are saying that your findings in your report including the figures that appear in Figure 2 and Figure 3 of your report, are relevant and applicable to the incident that occurred in this case, the exposure of the information by LabMD, because Mr. Boback testified in November 2013 that the insurance aging report could be found in multiple locations?" A. "Yes, because the insurance aging report could be found in multiple locations." Q. "At the time that he testified?" A. "At the time that he testified.");
(RX 523 (Van Dyke, Dep. at 109-110) (Q. "How is time a factor in your calculations other than 12 months from the time that the survey respondents responded?" A. ". . . we chose the time

period because Mr. Boback testified that the time that he most recently saw evidence of all those SSNs out there, that are likely to lead to identity fraud in my opinion, that time period fell within our 12–month measurement period.”)).

441. Van Dyke’s report and opinions at trial regarding ongoing identity theft or medical identity theft specifically relied upon Boback’s November 2013 testimony regarding the 1718 File and the Day Sheets. (Van Dyke, Tr. 645-646) (Q. “Would it matter if the 1718 File and the day sheets were in the hands of governmental entities?” A. “If that was an authorized party, in other words, not a data breach, then that would matter because the calculations wouldn't apply here. But that was not the case in this instance.” Q. “How do you know it wasn’t the case in this instance?” A. “Because, according to the testimony that I’ve read, the 600 day sheets were found in the possession of individuals that have pleaded no contest to identity theft. And in reading through Mr. Boback’s testimony as of late 2013, the 9300 PII records were found in as many as four locations, four IP locations, so that’s what I’m relying on, is his statement.” Q. “Are you aware of who owned those IP locations where the 1718 File was found?” A. “No. I’m relying on his testimony.”); (Van Dyke, Tr. 667-660) (Q. “I still don’t understand how the 30.5 percent figure relates to those individuals whose names appear on the 1718 File when those individuals were never notified of a data breach. . . .” A. . . . “That relates to the 1718 File because we know that the 1718 File, from the testimony of Mr. Boback, that it was found in four places where it didn’t belong, so that’s the indicator of the first thing, exposure of the data. And I use that to make an estimate, a projection -- pardon me -- of the amount of harm that those people who have had their data exposed in an unauthorized way are likely to encounter.”)).

442. Van Dyke disregarded the facts underlying how the 1718 File was taken from LabMD. (RX 523 (Van Dyke, Dep. at 39) (Q. “Were you told that it was a fact in this case, were

you told or did you see any information that you were provided that indicated that someone other than Tiversa had found the 1718 file outside of LabMD's possession?" A. "I don't believe so." Q. "In terms of your analysis does it matter how the insurance aging file was taken from LabMD?" A. "That's something I haven't considered in my opinion." Q. "In terms of your analysis would it matter how it was taken from LabMD?" A. "Again, I haven't give any consideration to that."); (Van Dyke, Tr. 645) (Q. ". . . In terms of arriving at your conclusions and your opinions, does it matter to you how the 1718 File and the day sheets escaped LabMD's possession?" A. "No, it does not matter to me.")).

443. Van Dyke's analysis failed to include any temporal component as regards the 1718 File, and assumed the same amount of damage would occur from the disclosure of the information regardless of whether it was available for two month or four years. (RX 523 (Van Dyke, Dep. at 41-42)) (Q. "So when the insurance aging file escaped the possession of LabMD did not figure into your considerations or analysis at all?" A. "No, not when it escaped." Q. "Does your analysis have a temporal component to it at all as it relates to the insurance aging file?" A. "No, it does not." Q. "So your analysis does not take into account the length of time that the information contained on the insurance aging file has been exposed to unauthorized third parties?" A. "No, it does not.").

444. Van Dyke's methodology and analysis as contained in his report and opinions is based on Javelin's 2013 ID Fraud Survey. (CX 0741 (Van Dyke, Rep. at 4); [redacted]

445. Javelin's 2013 Fraud ID Survey relied upon Knowledge Networks, which was a vendor paid by Javelin for the last four (4) years to provide access to survey respondents. (CX 0741 (Van Dyke, Rep. at 4 n.6); (RX 523 (Van Dyke, Dep. at 113-114)).

446. Van Dyke's report, opinions, and the 2013 Fraud ID Survey erroneously applied 2013 data to the facts of the 1718 File disclosure. (RX 523 (Van Dyke, Dep. at 96); (CX 0741 (Van Dyke, Rep. at 12 Fig. 3)).

447. The respondents' answer to Question 2 under Figure 1 of the Van Dyke report was confined to the 12-month period preceding the Survey, October 2013 back to October 2012. (Van Dyke, Tr. 655) (Q. "So we've got two time periods going on in that question; correct? One, been notified within the past twelve months; correct?" A. "Yes." Q. "And it's the past twelve months of responding to the survey." A. "That's correct." Q. "So the time period runs from the day the respondent responds to the survey twelve months back from that day; correct?" A. "That's right."); (CX 0741 (Van Dyke, Rep. at 8 Fig. 1)).

448. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the total one year fraud amount (in billions) for the years 2006 through and including 2012. [redacted]

449. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean fraud amount per fraud victim for the years 2006 through and including 2012. [redacted]

450. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the median fraud amount per fraud victim for the years 2006 through and including 2012. [redacted]

451. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean consumer cost for the years 2006 through and including 2012. [redacted]

452. The 2013 ID Fraud Report upon which Van Dyke relied in his report and opinions indicates a decrease in the mean resolution time (hours) for the years 2006 through and including 2012. [redacted]

453. The information contained in Figure 3 of the 2013 Fraud ID Report contradict and/or belie Van Dyke's report and opinions as to whether and to what extent consumers were at significantly higher risk of becoming victims of identity fraud and/or medical identity theft/fraud for the relevant time period in this case which is January 2005 to July 2010. (CX0741 (Van Dyke, Rep. at 3)); [redacted]

454. Van Dyke's report, opinions, and trial testimony relied upon the 2013 Ponemon Survey on Medical Identity Theft which was financed by Richard Kam's Company, ID Experts. (CX 0741 (Van Dyke, Rep. at 18)).

455. Van Dyke could not identify a single victim of identity theft or fraud, medical theft or fraud, or any consumer injury as a result of the 1718 File or the Sacramento Day Sheets. (CX 0741 (Van Dyke, Rep. at 1-21)).

456. Van Dyke's projection is erroneous that within one (1) year of unauthorized disclosure, 7.1% of the individuals on the 1718 File list should have experienced non-card identity fraud because victims of identity theft from the 1718 File and the Day Sheets do not exist. (Van Dyke, Tr. 692-693)) (Q. "***So if the information contained on the 1718 File was exposed in February of 2008, then sometime between February of 2008 and February of 2009,***

***7.1 percent of those individuals should have experienced existing non-card fraud." A. "That would be my projection, yes." Q. "Okay. And if the evidence is that none of those individuals experienced existing non-card fraud during that period of time, is there -- I mean, how would you explain that or could you explain it?" A. "I actually couldn't give you a response to that because what I'm solely relying on is, you know, the ten years of surveying these populations. Now we're over 5,000 people. . . . So I'm not really in a position to say – to somehow apply that in reverse. The research, I'm sorry, just wasn't designed to be used in that way and I – I couldn't in good conscience respond to that."*) (emphasis added).**

457. Van Dyke does not explain why none of the individuals notified by LabMD that their PII (Personal Identifying Information) had been disclosed to unauthorized persons became victims of identity fraud. (RX 523 (Van Dyke, Dep. at 70-71)) (Q. ". . . So is it your opinion then that 30.5 percent of the individuals who were notified by LabMD that their personal identifying information had been disclosed to unauthorized persons will become victims of identity fraud?" A. "Yes." Q. "And hypothetically if none of those individuals became victim[s] of identity fraud are there any factors that come to mind that might cause that to happen?" A. "It's just impossible for me to speculate on something like that, it just defies reason." Q. "Well, it would defy reason at least in your mind that that could even happen, wouldn't it?" A. "Yes.").

458. Van Dyke "assumed that LabMD failed to provide reasonable and appropriate security for the personally identifiable information maintained on its computer networks." (Van Dyke, Tr. 642); (CX 0741 (Van Dyke, Rep. at 2)).

459. Van Dyke assumed that the 1718 File and the Sacramento Day Sheets were found outside of LabMD as a result of a data breach. (Van Dyke, Tr. 678-679).

460. Van Dyke is not a statistician, yet his report relied upon a cross-tabulation technique which involves "comparison of statistical data." (Van Dyke, Tr. 673-675); (Van Dyke, Tr. 587) (Q. "Do you use cross-tabulation?" A. "Yes. Yeah. I might have -- it might be easier if I just said the method I was describing a moment ago was cross-tabulation." Q. "And what is cross-tabulation?" A. "So that's a -- within the research circle, that's a term that's widely used to describe statistical -- you know, comparison of statistical data.").

461. Van Dyke's definition of cross–tabulation is confusing and inconsistent. (Van Dyke, Tr. 587) (Cross–tabulation is the "comparison of statistical data."); (A. ". . . Cross-tabulation is just a universally accepted method among researchers for comparing two populations, people who have experienced two things. However, it is the same thing. . . .").

462. In reference to Figure 1 at page 8 of his report in this case, Van Dyke confuses cross–tabulation comparing data from selected survey years with cross–tabulation of data within a single survey year, which renders his testimony self–contradictory and unreliable. (Van Dyke, Tr. 650-651) (Q. "And in terms of utilizing cross-tabulation, do you do that to arrive at conclusions on the same survey or do you take information over a period of years and cross-tabulate it to come to conclusions?" A. "Oh. We would never -- if I'm understanding your question, we would never compare the results of individuals who respond in a particular way to -- within one survey -- and I need to be very careful about the way I'm communicating this -- with a set of respondents from another survey. In other words, we wouldn't mash the data together, so to speak. . . . Cross-tabulations were done within [Fig. 1 of my report], and we compared the results of that cross-tabulation to the results of a cross-tabulation in another survey." Q. "So another survey of the same kind for a different year." A. "Yes." Q. "Because if you look at figure 1, it appears that there's years 2010, 2011, 2012 and 2013 listed there;

correct?" A. "That's correct." Q. "So are you saying that these numbers for each year are the result of a cross-tabulation?" A. "Within each year."); (CX 0741 (Van Dyke, Rep. at 8 (Fig. 1)).

463. Van Dyke testified that cross–tabulation and extrapolation "are different things" and extrapolation is "more accurate" in his opinion. (Van Dyke, Tr. 673-674) (JUDGE CHAPPELL: "What's the difference in cross-tabulation and extrapolation?" THE WITNESS: "Yeah, those are different things. So extrapolation is a process of reaching a conclusion, and so it might include just logic or just a wide variety of methods. But cross-tabulation is a statistician's method of precisely comparing, taking a subset of another, essentially doing division." JUDGE CHAPPELL: "Which is more accurate?" THE WITNESS: "A cross-tabulation would be more accurate, Your Honor." BY MR. SHERMAN: Q. "But you're not a statistician; correct?" A. "I'm not personally a statistician, no.").

464. Van Dyke never surveyed anyone from the 1718 File for purposes of his report, opinions, and testimony in this case. (Van Dyke, Tr. 677-678).

465. Van Dyke extrapolated the information in the 2013 Fraud ID Survey and overlaid data over the information from the 1718 File and the Sacramento Day Sheets. (Van Dyke, Tr. 676-677).

466. Van Dyke admitted that he never considered any of the specific facts of the case. (CX 0741 (Van Dyke, Rep. at 72-73)).

467. Van Dyke did not account for type of breach or who gained the information. (RX 523 (Van Dyke, Dep. at 42-43, 58)).

468. Van Dyke assumed that the same amount of damage would occur from the disclosure of the information regardless of how long it was available on a peer to peer network. (RX 523 (Van Dyke, Dep. at 41)).

L. <u>Professor Shields.</u>

469. Complaint Counsel did not proffer an expert witness with respect to P2P networks or LimeWire. (Tr. 747-748).

470. Professor Clay Shields ("Shields") testified as a rebuttal witness *only*. (Tr. 747-748).

471. Shields confirmed Fisk's testimony that once an ultrapeer discovers that another peer (computer) is behind a firewall, which it finds out when it initially runs a search, the ultrapeer is "able to test its network connection and determine if there's a firewall. If it determines there's a firewall, it finds . . . [another of the] ultra peers that's outside the firewall that's able to act on its behalf." (Shields, Tr. 841-842) (confirming Fisk's expert testimony).

472. Professor Shields was not able to find the 1718 File on the Gnutella network as he wrote his rebuttal expert report or prepared to testify. (Shields, Tr. 892).

473. Professor Shields does not have much, if any, experience with LimeWire. (Shields, Tr. 893).

474. Professor Shields does not know how the LabMD 1718 File was "actually shared," obtained by Tiversa, or if or how the 1718 File got on the network. (Shields, Tr. 904-07).

475. Professor Shields' opinions were based on the deposition of Boback and he assumed that the 1718 File had been shared and made available over Gnutella on the LimeWire network. (Shields, Tr. 904-06).

476. Computers with firewalls cannot be ultrapeers. (Shields, Tr. 909).

477. Finding one particular file on the internet by use of LimeWire is sort of like the lottery. (Shields, Tr. 917).

478. A file, like the 1718 File, that includes the lettered series of "insuranceaging" cannot be found by a LimeWire search for the term "insurance." (Shields, Tr. 917-18).

M. Complaint Counsel's Proofs.

479. There is no perfect security. (CX 0721 (Johnson, Dep. at 25, 38, 90); (RX 524 (Hill, Dep. at 149)).

480. Complaint Counsel introduced any evidence that any of LabMD's alleged unfair data security acts or practices, even taken together, "causes" substantial injury to consumers or harm to competition. (Tr. 1-1486); (CX 0001 – CX 0878).

481. Complaint Counsel has not introduced any evidence that LabMD's pre-July 2010, data security acts or practices are continuing or that such wholly past acts or practices "likely to cause" future harm, almost six years after the fact. (Tr. 1-1486); (CX 0001 – CX 0878).

482. Complaint Counsel has not introduced any evidence or proven that the 1718 File has been obtained by anyone other than Tiversa, Johnson, Dartmouth and FTC, or that it was available via LimeWire at LabMD after May 2008, approximately seven and one-half years ago. (Tr. 1-1486); (CX 0001 – CX 0878).

483. The 1718 File was taken by Tiversa on February 25, 2008, and subsequently disclosed to Johnson, Dartmouth and FTC. (Wallace, Tr. 1441-1442, 1358-1364); (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 8, 11-12)).

485. The 1718 File was not obtained, reviewed, or disclosed by any other person, except by the intentional actions of Boback, Wallace, Tiversa, Johnson, Dartmouth, and FTC. (Wallace, Tr. 1441-1442, 1358-1364); (CX 0382 (Article: Data Hemorrhages in the Health-Care Sector, at 8, 11-12)).

486. The 1718 File was not available via LimeWire from LabMD after May 2008. (RX 097 – RX 118 (Daily IT Walk) (May 2008 – July 2008); (RX 119 – RX 169 (LabMD email re: walk arounds) (Mar. 2009 – Aug. 2009); (RX 174 – RX 264 (LabMD email re: walk arounds) (Aug. 2007 – July 2008)).

484. No consumer has suffered monetary or reputational harm due to the "Security Incidents" described in the Complaint. (Tr. 1-1486); (CX 0001 – CX 0878).

485. Complaint Counsel has not introduced evidence that consumers who receive notice of a data breach not reasonably capable of mitigating the injury. (Tr. 1-1486); (CX 0001 – CX 0878).

486. Complaint Counsel seeks to declare wholly past conduct in this case unfair and unlawful. (Complaint (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357), at 1-12 ¶¶ 1-23, Appendix A (13-57)).

487. Complaint Counsel did not introduce any evidence the allegation in ¶4 of the Complaint, that "[c]onsumers ***in many instances*** pay respondent's charges with credit cards or personal checks" is now true or was so with regard to any of the specific individuals in the 1718 File or the Day Sheets. (Tr. 1-1486); (CX 0001 – CX 0878).

489. Complaint Counsel did not introduce any evidence regarding the allegation in ¶6 of the Complaint, that LabMD "routinely obtains information about consumers," is now true. The evidence is LabMD has not obtained information about consumers since January, 2014. (CX0291 (LabMD Letter to Physicians Offices re: Closing); (Tr. 1-1486); (CX 0001 – CX 0878)).

490. LabMD does not operate a computer network. (CX0291 (LabMD Letter to Physicians Offices re: Closing)).

491. LabMD's billing department does not use the computer networks to generate or access documents related to processing copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers. (CX0291 (LabMD Letter to Physicians Offices re: Closing)).

492. Complaint Counsel did not introduce any evidence regarding the allegation in ¶10 of the Complaint that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." (Tr. 1-1486); (CX 0001 – CX 0878).

493. LabMD used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. (RX 533 (Fisk, Rep. at 3-4, 6-34, 37); (45 C.F.R. Part 160 and Part 164, Subparts A and C (HHS Security Rule), at § 164.302, § 164.308(a)(1), § 164.312(a)(1); (HIPAA Security Series (**7 Security Standards: Implementation for the Small Provider**) (VOL. 2/Paper 7) (Dec. 10, 2007), 1-3 ("***Factors that determine what is 'reasonable' and 'appropriate' include cost, size, technical infrastructure and resources.***") (emphasis added), 12 (***"The scalable, flexible and technology neutral principles of the Rule allow covered entities to comply in a manner consistent with the complexity of their particular operations and circumstances. Small covered healthcare providers should use this paper and other applicable resources to review and maintain their Security Rule compliance efforts."***) (emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf (last accessed Aug. 9, 2015); (Health Insurance Portability and Accountability Act of 1996 Pub. L. No.104–191, § 1173(d)(1)(A)(v), 110 Stat. 1936, 2026 (1996)); (60 Fed. Reg. 8335 (Feb. 20,

2003) (codified at 45 C.F.R. pts. 160, 162, & 164) (2007)); (Dep't of Health & Human Servs. (HIPAA Security Series (**6 Basics of Risk Analysis and Risk Management**) (Volume 2/ Paper 6) (6/2005: rev. 3/2007), 3)) ("…only federal agencies are required to follow federal guidelines like the NIST 800 series … Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations.") (italic emphasis in original) (bold emphasis added), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf (last accessed Aug. 9, 2015)).

494. LabMD required employees and doctors to use common authentication-related security measures. (RX 533 (Fisk, Rep. at 16-22); (RX 071 (LabMD Employee Handbook); (CX 0005 (LabMD Compliance Program); (RX 075 – RX 095 (LabMD Acceptable Use and Security Policy); (CX 0130 (LabMD Employee Handbook)).

495. Complaint Counsel did not introduce any evidence regarding the allegation in ¶11 of the Complaint that LabMD "could have corrected its security failures at relatively low cost using readily available security measures." (Tr. 1-1486); (CX 0001 – CX 0878).

496. Complaint Counsel did not introduce any evidence regarding the allegation in ¶12 of the Complaint that LabMD's "[c]onsumers have no way of ***independently knowing*** about respondent's [alleged] security failures and ***could not reasonably avoid possible harms*** from such [alleged] failures, including identity theft, medical identity theft, and other harms, such as

disclosure of sensitive, private medical information." (Tr. 1-1486); (CX 0001 – CX 0878) (emphasis added).

497. LabMD is subject to the HIPAA Breach Notification Rule and has complied with it in the past – the FTC has admitted that LabMD has always complied with HIPAA/HITECH data-security standards. (CX 0679 *(LabMD v. FTC*, Verified Complaint for Declaratory and Injunctive Relief (N.D. Ga.), Ex. 12 at p. 13)).

498. Complaint Counsel offered no testimony or other evidence this Rule was inadequate. (Tr. 1-1486); (CX 0001 – CX 0878).

499. The Commission did not warn businesses about the risk of inadvertent file sharing until January 2010, at the earliest. (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

500. The 1718 File was not generally available on a P2P network through LimeWire, a P2P file sharing application. (Wallace, Tr. 1361-1444); (Fisk, Tr. 1153) ("So in the case of the insurance aging file, . . . [the program was] not intelligent enough to separate 'insurance' from 'aging,' so it [would] just take 'insurance' -- it [would] see that underscore and it [would see] 'insuranceaging' as one big keyword, and then it [would] actually do what's called a little bit of prefix matching on that, on that keyword. So once it's identified 'insuranceaging' as a keyword, it [would] then strip off the final characters of up to three, so it [would] enter 'insuranceaging' as the keyword, and then it will enter 'insuranceagin' without the 'g' and then 'insuranceagi' without the 'n' and the 'g' and 'insuranceag' without the 'ing' as all – as separate, as separate keywords. And then it [would] also enter the numbers as keywords as well."); (Fisk, Tr. 1156).

498. Complaint Counsel offered no testimony that consumers, upon receiving notice, were anything other than reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact. (Tr. 1-1486); (CX 0001 – CX 0878).

499. Complaint Counsel did not introduce any evidence regarding the allegation in ¶15 of the Complaint that "[g]enerally, once shared, a file cannot with certainty be removed permanently from a P2P network." (Tr. 1-1486); (CX 0001 – CX 0878).

500. Complaint Counsel did not introduce any evidence regarding the allegation in ¶16 of the Complaint that "[s]ince at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks." (Tr. 1-1486); (CX 0001 – CX 0878).

502. The Commission did not warn businesses about the risk of inadvertent file sharing until January 2010. (Inadvertent File Sharing Over Peer-To-Peer Networks: Hearing Before the H. Comm. on Oversight and Gov't Reform, 110th Cong., 1st Sess. 1, 10, 40-84 (July 24, 2007), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg40150/html/CHRG-110hhrg40150.htm (last accessed Aug. 9, 2015) ("The [2005 FTC Report] emphasized that many of the risks posed by P2P file sharing also exist when consumers engage in other Internet-related activities, such as surfing Web sites, using search engines, or e-mail.…")); (FTC Staff Report, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, 20 (June 2005), *available at* http://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (last accessed Aug. 9, 2015) ("***Although it has required warnings with respect to inherently dangerous products, the Commission concluded that it was not aware of any basis under the FTC Act for requiring warnings for P2P file sharing and other neutral consumer***

technologies.") (emphasis added); (Fed. Trade Comm'n, Widespread Data Breaches Uncovered by FTC Probe (Feb. 22, 2010), *available at* https://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe (last accessed Aug. 9, 2015)).

501. Complaint Counsel has failed to prove by a preponderance of the evidence the allegations in ¶¶17-18 of the Complaint that LabMD's insurance aging file was generally available on a P2P network through Limewire, a P2P file sharing application. (Wallace, Tr. 1361-1444).

502. LabMD did not knowingly violate Section 5. (RX 052 (Email between Boyle and Tiversa); (RX 053 (Email between Boyle, Daugherty, and Tiversa); (RX 054 (Email between Boyle and Tiversa); (RX 055 (Email between Boyle and Tiversa); RX 056 (Email between Boyle and Tiversa); RX 057 (Email between Boyle and Tiversa); (RX 058 (Email between Boyle and Daugherty re: breach); (Daugherty, Tr. 985-987)).

503. Complaint Counsel has not alleged or proven LabMD is a serial violator of Section 5. (Tr. 1-1486); (CX 0001 – CX 0878).

504. FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices, stating that LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

505. FTC did not name an individual complainant or allege direct harm to any identifiable person, and FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively

low cost." (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

506. FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," and at any given point in time, allegedly violated Section 5. (Complaint, at 1-5 ¶¶ 3-21 (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357)).

N. The Damage Done To LabMD

507. LabMD provided a unique, useful and important service to doctors and their

patients. (Daugherty, Tr. 493, 944-945, 955-964); (Daugherty, Tr. 962) (A. "And in our marketplace, typically approximately 85 percent of all the specimens were allowed to come to LabMD. But that 15 percent that weren't allowed to come to LabMD, by removing all the pitfalls of having to manage that was a huge time savings and a huge removal of bureaucracy from physicians' offices. . . . the amount of errors just fell through the floor. . . . [W]e even knew ahead of time what was coming so that we could be prepared.").

508. The Commission's inquisition substantially interfered with LabMD's operations.

(Daugherty, Tr. 1028-1034).

509. LabMD criticized FTC and Commission staff. (Respondent LabMD's Motion to

Dismiss the Complaint With Prejudice (*In the Matter of LabMD, Inc., a corporation*, FTC No. 9357) at 30 n.23)) ("Notably, the Complaint (along with a FTC press release making disparaging claims about LabMD) was issued shortly before publication of LabMD's CEO's book, *The Devil Inside the Beltway*, in which he exercises his First Amendment right to speak candidly about a matter of public concern and criticizes Complaint Counsels' actions and the Commission's treatment of LabMD in great detail. Complaint Counsels' burdensome and oppressive discovery requests—which run afoul of norms of conduct that obtain in Article III courts and *flagrantly* violate Fed. R. Civ. P. 30(a)(2)(A)'s limits on depositions—followed shortly after the book's publication. The First Amendment prohibits government agencies from retaliating against private citizens for engaging in constitutionally protected speech by bringing baseless enforcement actions. *See Trudeau v. FTC*, 456 F.3d 178, 190-91 nn.22-23 (D.C. Cir. 2006))." (emphasis in original).

510. The Commission brought a complaint against LabMD in August, 2013, after LabMD had publicly criticized FTC and its staff in very strong terms. (Daugherty, Tr. 1027).

511. At that time [August 2013], the Commission did not have evidence that any

consumer had suffered monetary harm or other harm due to the Security Incidents. (Complaint, *In the Matter of LabMD, Inc., a corporation*, at 1-12, Appendix A (13-57)).

512. At that time, the Commission did not have evidence LabMD's post July, 2010,

data security acts or practices were inadequate or unreasonable. (Complaint, In the Matter of LabMD, Inc., a corporation, at 1-12, Appendix A (13-57)).

513. LabMD's pre-July 2010 data security acts or practices changed over time and

could not reoccur. (Tr. 1-1486); (CX 0001 – CX 0878).

514. In or about August 2013, the Commission knew or should have known that the

1718 File had been obtained only by and was available only to Tiversa, Johnson, Dartmouth and FTC. (Complaint, In the Matter of LabMD, Inc., a corporation, at 1-12, Appendix A (13-57)).

515. For three and one-half months, Commission staff did not inform LabMD that FTC had possession of the Day Sheets. However, Commission staff knew or should have known LabMD had an obligation under HIPAA to give notice of the unauthorized disclosure of PHI or PII. (Daugherty, Tr. 1027-1028) (Q. "What is it that you contend that the Federal Trade Commission didn't tell you?" A. "They didn't tell us they had the day sheets for three and a half months, even though we're subject to HIPAA, which requires us to notify in 60 days. . . . On the one hand we're supposed to protect patients and we're supposed to follow the law, and yet the federal government is withholding information from us, so it seems to me they're more eager to lambaste us and entrap us than keep patients safe. So we were outraged, scared, felt entrapped, and employees were starting to really break under pressure when that went down.").

516. FTC's actions in this case destroyed morale, attention, and energy at LabMD. (Daugherty, Tr. 1028) (Q. "What other impacts did it have on LabMD's business?" A. ". . . I can't understate how damaging and confusing and sideswiping this was to the attention, energy and morale of the management staff that knew because we, you know, had a company to run....").

517. FTC's actions in this case destroyed LabMD's client base generally by attrition and innuendo, and specifically by Complaint Counsel's serving subpoenas upon and deposing LabMD's employees, clients, client–physicians, and third–party vendors. (Daugherty, Tr. 1029-1031) (Q. "Was there any impact on the business externally?" A. "Yes." Q. "And what was

that?" A. "Well, the press broke the story in 2012, so once the press broke the story, . . . you can't control perception, and so I had physicians upset with me they didn't hear it from myself. I had people concerned . . . The negative external impact on LabMD's business reputation, income, and ability to keep and maintain clients, employees, and third-party vendors was exacerbated by the fact that "most people in medicine don't know what the FTC is" because the FTC does not regulate data security or anything else in the medical industry."); (Daugherty, Tr. 1029-1030) (Q. "Was there any impact on the business externally?" A. "Yes." Q. "And what was that?" A. ". . .I did find out later, for example, the rumor had twisted around so that -- because, you know, most people in medicine don't know what the FTC is, so I'm getting told, I hear you're in trouble with the SEC about some trade -- I mean, just the rumors just went crazy.").

518. In or about November 13, 2013, however, Commission staff knew or should have

known Tiversa and Boback had committed perjury with respect to claims of spread reflected on CX 0019. (CX 0307 (Privacy Institute Spreadsheet with IP Address); (CX 0019 (Tiversa: List of 4 IP Addresses where Insurance Aging File found); (Wallace, Tr. 1344-1347, 1352-1354, 1358-1374, 1378-1385)).

519. As of May 27, 2014, LabMD's operations were operational only for the purposes of maintaining tissue samples for LabMD's physician-clients and the patients they jointly serve. (Daugherty, Tr. 1031) (Q. "Mr. Daugherty, what is the current state of LabMD's operations?" A. "LabMD is in a very deep coma. We are still in business. The corporation is still standing. I'm the only employee. All we do -- we preserve the slides and the electronic data for the physicians so they can still get results if they don't have them and they can still send slides out

for second opinions. Because that goes on, you know, that doesn't just stop. . . . prostate cancer is a very slow-growing disease, so you can have it for 14 years, . . . and there's technologies [that are] available now to analyze versus what was available five years ago [on] aggressiveness of the tumor cells, so we keep all that available still."); (CX 0291 (LabMD Letter to Physicians' Offices re: Closing) (". . . First and foremost, even during this closure, patient care is still priority number one with LabMD . . .")).

520. As a result of FTC's actions in this case, LabMD was sued by its landlord for approximately $900,000.00 for early termination of its lease. (Daugherty, Tr. 1031-1032).

521. As a result of FTC's actions in this case, LabMD has lost all primary insurance coverage for its employees as well as its malpractice insurance for both LabMD's physician–employees and its facility. (Daugherty, Tr. 1032-1033) (Q. "What's the state of LabMD's insurance coverage?" A. "Well, in the beginning, we of course had medical insurance, dental insurance, workmen's comp, vision, general liability, medical malpractice for the physicians, medical malpractice for the facility. So of course we had to let everybody go. They still have dental and medical through COBRA should they choose at their expense. The vision is gone. The workmen's comp is gone. . . . [The] general liability for the corporation has been nonrenewed because of the Federal Trade Commission action and claims.[]" Q. "How do you know that's the reason?" A. "Because they told us. The medical malpractice -- when you close -- obviously we're not practicing medicine now and moving forward, so the medical malpractice is for tail coverage for any claims -- any claims from any practiced medicine we did in the last few years would be covered in the future for the next couple of years. We had carriers that flat-out would deny to quote us because of the Federal Trade Commission investigation, even though, you know, these are medical malpractice. I don't think that the Federal Trade

Commission has any jurisdiction over medical malpractice. . . . but [the malpractice carriers] didn't care. . . . I got tail coverage for the physicians, and there were many fewer insurance carriers that were willing to quote it. But we did get insurance [] tail coverage for the two physicians that we had to let go.").

522. As a result of the FTC's actions in this case, LabMD sent a letter dated January 6, 2014 to its administrators, physicians, nurses, and "valuable support staff" stating that the last day patient specimens would be accepted at the facility would be Saturday, January 11, 2014. (CX 0291 (LabMD Letter to Physicians Offices re: Closing)) (". . . It is with deep regret and sadness I am writing you to announce that the last day LabMD will be accepting new specimens is Saturday, January 11, 2014. . . .").

523. In its letter dated January 6, 2014, LabMD stated that the reason for its actions in shutting down its facility was "the conduct of the [FTC]" in that the FTC's actions "subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data–security vulnerability." (CX 0291 (LabMD Letter to Physicians Offices re: Closing)) ("The FTC has subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data–security vulnerability. Without standards, information, or Congressional approval, and without a customer victim from the alleged 'breach,' the FTC has taken it upon itself to spend your tax dollars to ruin LabMD and regulate medical data security over and above HIPAA. LabMD's fight with the FTC has become, as Government Health IT stated, ". . . a dispute that could shape the future of health privacy regulation.' In other words, this is a very big deal that may result in another regulator, without expertise or clear standards, standing over your shoulder with the power to destroy your practice or your company.")

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

Counsel for Respondent

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

Counsel for Respondent, LabMD, Inc.

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

ATTACHMENT 1

IN THE MATTER OF
LABMD, INC
DOCKET NO. 9357

RESPONDENT COUNSEL'S EXHIBIT INDEX

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX001	6/1/07 Day Sheet Transaction Details	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1011; 1013-1019; 1021-1033; 1071-1078		CX0687
RX002	Insurance company web access sheet	JX 2 see Tr. 6:15-16			
RX003	IT Staff Checklist	JX 2 see Tr. 6:15-16			
RX004	website list	JX 2 see Tr. 6:15-16			
RX005	windows screenshot	JX 2 see Tr. 6:15-16			
RX006	Sentinel Network Complaint	JX 2 see Tr. 6:15-16			CX0402
RX007	FTC envelop scan	JX 2 see Tr. 6:15-16			CX0441
RX008	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0491
RX009	Service Solutions Proposal for LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0047
RX010	Email from H. Davidson to M. Daugherty dated	JX 2 see Tr. 6:15-16			
RX011	Service Solutions Proposal for LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX012	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX013	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0048
RX014	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0049
RX015	Invoice to LabMD from ProviDyn, Inc.	JX 2 see Tr. 6:15-16			CX0050
RX016	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX017	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX018	Calendar Meeting Request	JX 2 see Tr. 6:15-16			
RX019	Letter from Mike Daugherty to ProviDyn, Inc.	JX 2 see Tr. 6:15-16			
RX020	Service Solutions Proposal for LabMD from ProviDyn	JX 2 see Tr. 6:15-16			
RX021	Service Solutions Proposal for LabMD from ProviDyn	JX 2 see Tr. 6:15-16			CX0051
RX022	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0055
RX023	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX024	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0057
RX025	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0059
RX026	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0061

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX027	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0062
RX028	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0063
RX029	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0064
RX030	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0065
RX031	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX032	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX033	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX034	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX035	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX036	Full Report Analysis	JX 2 see Tr. 6:15-16			
RX037	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0066
RX038	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0072
RX039	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0073
RX040	Full Report Analysis	JX 2 see Tr. 6:15-16			CX0074
RX041	Email from J. Boyle to R. Boback re: Breach Notification	JX 2 see Tr. 6:15-16			
RX042	Rapid SSL ad	JX 2 see Tr. 6:15-16			CX0135
RX043	Rapid SSL FAQ	JX 2 see Tr. 6:15-16			
RX044	TrendMicro ad	JX 2 see Tr. 6:15-16			
RX045	Cyprus Communications Services Order	JX 2 see Tr. 6:15-16			CX0253
RX046	Managed Data Solutions Invoice	JX 2 see Tr. 6:15-16			CX0264
RX047	MediPro Sale Invoices	JX 2 see Tr. 6:15-16			
RX048	MediPro Sales Invoice	JX 2 see Tr. 6:15-16			
RX049	MediPro Sales Invoice	JX 2 see Tr. 6:15-16			
RX050	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX051	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX052	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16	Daugherty, Tr. 985-987		
RX053	Email between Boyle, Daugherty, and Tiversa	JX 2 see Tr. 6:15-16			
RX054	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX055	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX056	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX057	Email between Boyle and Tiversa	JX 2 see Tr. 6:15-16			
RX058	Email between Boyle and Daugherty re: breach	JX 2 see Tr. 6:15-16			
RX059	Email between Boyle and Tiversa re: breach	JX 2 see Tr. 6:15-16			
RX060	Mail Batch Instructions	JX 2 see Tr. 6:15-16			CX0162
RX061	Daily Credit Card Transactions Form	JX 2 see Tr. 6:15-16			CX0233
RX062	LabMD New Team Member Checklist	JX 2 see Tr. 6:15-16			CX0003

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX063	Patient Aging Report	JX 2 see Tr. 6:15-16			CX0163
RX064	Rose Bellvue 2008 Performance eval	JX 2 see Tr. 6:15-16			
RX065	LabMD Staff Responsibility breakdown	JX 2 see Tr. 6:15-16			CX0234
RX066	Jan 2007 Monthly Status of Pending Tasks Form	JX 2 see Tr. 6:15-16			CX0119
RX067	List of clients with remote access to LabMD system	JX 2 see Tr. 6:15-16			CX0134
RX068	LabMD Performance Eval Form	JX 2 see Tr. 6:15-16			
RX069	LabMD Insurance Aging Report	JX 2 see Tr. 6:15-16			CX0165
RX070	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0005
RX071	LabMD Employee Handbook	JX 2 see Tr. 6:15-16	Hill, Tr. 288-295		
RX072	LabMD Insurance Aging Report (1718 file)	JX 2 see Tr. 6:15-16			CX0166
RX073	Certification page signed by Daugherty	JX 2 see Tr. 6:15-16			
RX074	LabMD Computer Hardware and Security Manual	JX 2 see Tr. 6:15-16			
RX075	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX076	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX077	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX078	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX079	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX080	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX081	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX082	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX083	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX084	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX085	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX086	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX087	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX088	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX089	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX090	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX091	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX092	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX093	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX094	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX095	LabMD Acceptable Use and Security Policy	JX 2 see Tr. 6:15-16			
RX096	Server Ports and Firewall Mapper	JX 2 see Tr. 6:15-16			CX0178
RX097	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX098	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX099	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX100	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX101	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX102	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX103	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX104	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX105	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX106	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX107	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX108	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX109	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX110	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX111	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX112	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX113	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX114	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX115	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX116	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX117	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX118	Daily IT Walk	JX 2 see Tr. 6:15-16			
RX119	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX120	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX121	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX122	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX123	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX124	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX125	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX126	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX127	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX128	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX129	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX130	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX131	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX132	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX133	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX134	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX135	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX136	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX137	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX138	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX139	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX140	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX141	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX142	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX143	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX144	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX145	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX146	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX147	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX148	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX149	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX150	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX151	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX152	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX153	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX154	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX155	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX156	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX157	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX158	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX159	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX160	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX161	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX162	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX163	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX164	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX165	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX166	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX167	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX168	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX169	LabMD email re: walk arounds	JX 2 see Tr. 6:15-16			
RX170	TrendMicro Daily Virus Report	JX 2 see Tr. 6:15-16			CX0185
RX171	LabMD Virus Log	JX 2 see Tr. 6:15-16			
RX172	LabMD Policy Manual	JX 2 see Tr. 6:15-16			CX0006
RX173	LabMD IT Staff Walkaround Checklist	JX 2 see Tr. 6:15-16			CX0004
RX174	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX175	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX176	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX177	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX178	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX179	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX180	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX181	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX182	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			CX0236
RX183	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX184	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX185	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX186	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX187	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX188	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX189	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX190	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX191	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX192	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX193	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX194	LabMD email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX195	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX196	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX197	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX198	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX199	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX200	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX201	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX202	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX203	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX204	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX205	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX206	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX207	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX208	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX209	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX210	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX211	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX212	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			CX0199
RX213	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX214	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX215	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX216	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX217	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX218	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX219	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX220	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX221	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX222	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX223	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX224	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX225	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX226	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX227	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX228	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX229	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX230	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX231	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX232	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX233	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX234	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX235	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX236	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX237	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX238	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX239	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX240	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX241	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX242	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX243	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX244	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX245	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX246	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX247	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX248	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX249	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX250	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX251	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX252	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX253	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX254	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX255	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX256	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX257	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX258	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX259	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX260	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX261	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX262	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX263	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX264	LabMd Email re: Daily IT Rounds	JX 2 see Tr. 6:15-16			
RX265	ZyXel Firewall Rules Storage Space in Use	JX 2 see Tr. 6:15-16			CX0257
RX266	LabMD Server Room Security Chart - Jun 2010	JX 2 see Tr. 6:15-16			
RX267	LabMD Server Room Security Chart - Jul 2010	JX 2 see Tr. 6:15-16			
RX268	Malware Quickscan Log	JX 2 see Tr. 6:15-16			CX0268
RX269	Malware Quickscan Log	JX 2 see Tr. 6:15-16			CX0818
RX270	Malware Bytes Scanner	JX 2 see Tr. 6:15-16			
RX271	Security scan results	JX 2 see Tr. 6:15-16			CX0825
RX272	Security Scan Results	JX 2 see Tr. 6:15-16			CX0830
RX273	Product Key Chart	JX 2 see Tr. 6:15-16			CX0169
RX274	July 2010 Security Scan List	JX 2 see Tr. 6:15-16			CX0193
RX275	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX276	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX277	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX278	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX279	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX280	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX281	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX282	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX283	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX284	Desktops/Servers Virus Summary	JX 2 see Tr. 6:15-16			
RX285	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX286	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX287	TrendMicro Daily Virus Report - July 2010	JX 2 see Tr. 6:15-16			
RX288	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX289	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX290	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX291	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX292	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX293	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX294	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX295	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX296	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX297	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX298	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX299	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX300	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX301	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX302	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX303	Malware Quickscan Log	JX 2 see Tr. 6:15-16			
RX304	Malware Quickscan Log	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX305	LabMD Employee Separation Agreement - Patrick Howard	JX 2 see Tr. 6:15-16			
RX306	Automated PC Technologies New Service Agreement	JX 2 see Tr. 6:15-16			CX0395
RX307	APT Service Invoice	JX 2 see Tr. 6:15-16			CX0035
RX308	Christopher Maire resume	JX 2 see Tr. 6:15-16			CX0203
RX309	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0005
RX310	LabMD Compliance Training Powerpoint	JX 2 see Tr. 6:15-16			CX0127
RX311	LabMD Employee Handbook acknowledgment page-Woodson	JX 2 see Tr. 6:15-16			
RX312	Email between Sandra Brown and John Boyle re: Limewire issues	JX 2 see Tr. 6:15-16			CX0170
RX316	Pathology Records and Materials Retention	JX 2 see Tr. 6:15-16			CX0834
RX317	Managed Data Solutions Security Scan Summary	JX 2 see Tr. 6:15-16			CX0046
RX318	LabMD connections map for Power Ferry Rd location- 2009	JX 2 see Tr. 6:15-16			CX0039
RX319	LabMD connections map for Power Ferry Rd location- 2010	JX 2 see Tr. 6:15-16			CX0040
RX320	LabMD connections map for Power Ferry Rd location- 2011	JX 2 see Tr. 6:15-16			CX0041
RX321	Juniper Networks Product Descriptions	JX 2 see Tr. 6:15-16			CX0835
RX322	Brandon Bradley resume	JX 2 see Tr. 6:15-16			CX0320
RX323	Monthly Computer Inspection Report	JX 2 see Tr. 6:15-16			
RX324	LabMD Serverroom virus scan - July 2010	JX 2 see Tr. 6:15-16			
RX325	Managed Data Solutions Project Proposal	JX 2 see Tr. 6:15-16			CX0194
RX326	Managed Data Solutions Project Proposal	JX 2 see Tr. 6:15-16			CX0195
RX327	Tiversa folder screenshot	JX 2 see Tr. 6:15-16			CX0149; CX CX0151; CX
RX328	LabMD folder screenshot	JX 2 see Tr. 6:15-16			CX0153
RX329	Limewire screenshot	JX 2 see Tr. 6:15-16			CX0154; CX CX0156
RX330	Insurance Aging pdf window screenshot	JX 2 see Tr. 6:15-16			CX0157
RX331	SacPD Netanalysis re: Maldonado and Garcia	JX 2 see Tr. 6:15-16			CX0101
RX332	Letter to M. Cox from R.J. Maxay	JX 2 see Tr. 6:15-16			CX0225
RX333	Letter to M. Cox from A.C. Troutman	JX 2 see Tr. 6:15-16			
RX334	LabMD Compliance Program	JX 2 see Tr. 6:15-16			CX0129
RX335	Confidentiality Agmt. Between LabMD and Deanna Bagwell Dated 3/23 (no year)	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX336	LabMD Employee Handbook	JX 2 see Tr. 6:15-16			CX0130
RX337	Form Letter from LabMD to affected patients	JX 2 see Tr. 6:15-16			
RX338	Handbook Receipt Signed By Adnan Savera	JX 2 see Tr. 6:15-16			
RX339	Email From J. Boyle To mdort@aol.com	JX 2 see Tr. 6:15-16			
RX340	Emai From J. Boyle To mikelabmd@gmail.com; mdort@aol.com	JX 2 see Tr. 6:15-16			
RX341	Email From G. Schultz to R. Boback	JX 2 see Tr. 6:15-16			
RX342	Email from J. Boyle to W. Hardin re: Preventative Maintenance	JX 2 see Tr. 6:15-16			
RX343	Email from W. Hardin to J. Boyle re: preventative maintenance	JX 2 see Tr. 6:15-16			
RX344	LabMD "Network Invent" summary	JX 2 see Tr. 6:15-16			CX0397
RX345	Automated PC Technologies Invoice	JX 2 see Tr. 6:15-16			CX0398
RX346	Email from R. Yodaiken to K. Jestes re: contact with the FBI	JX 2 see Tr. 6:15-16			
RX347	Email from K. Jestes to M. Wood re: RedactedLabMdsLetter	JX 2 see Tr. 6:15-16			
RX348	LabMD Patient Notification Letter [redacted]	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1019-1021		
RX349	Email from A. Sheer to K. Jestes re: Hi Karina - The package arrived safe and sound. Alain.	JX 2 see Tr. 6:15-16			
RX350	Email from K. Jestes to A. Sheer re: LabMD	JX 2 see Tr. 6:15-16			
RX351	Email from A. Sheer to K. Jestes re: LabMD from Sacrameno Police	JX 2 see Tr. 6:15-16			
RX352	Email from R. Yodaiken to K. Jestes re: LabMD	JX 2 see Tr. 6:15-16			
RX353	Email from R. Yodaiken to K. Jestes re: my first phone call	JX 2 see Tr. 6:15-16			
RX354	Email from A. Sheer to K. Jestes re: my first phone call	JX 2 see Tr. 6:15-16			
RX355	Clinical Laboratory Licenses	JX 2 see Tr. 6:15-16			
RX356	Unofficial protocol for document transmission between LabMD and Midtown Urology	JX 2 see Tr. 6:15-16			
RX357	LabMD closure announcement	JX 2 see Tr. 6:15-16			
RX358	LabMD Billing Patient Education article	JX 2 see Tr. 6:15-16			
RX359	Fusco Letter to Dartmouth	JX 2 see Tr. 6:15-16			
RX360	S. Fusco Letter to E. Johnson	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX361	S. Fusco Letter to Tiversa	JX 2 see Tr. 6:15-16			
RX362	LabMD IT project outline	JX 2 see Tr. 6:15-16			CX0313
RX363	Email from J. Boyle to M. Daugherty re: Your Passwords	JX 2 see Tr. 6:15-16			
RX364	J. Boyle email to M. Daugherty re: Hyer Software request	JX 2 see Tr. 6:15-16			
RX365	Email from C. Gormley to E. Johnson re: Aids clinic ppt	JX 2 see Tr. 6:15-16			
RX366	Aids clinic names/ssn chart	JX 2 see Tr. 6:15-16			
RX367	Email from C. Gormley to E. Johnson re: Are you...	JX 2 see Tr. 6:15-16			
RX368	Email from C. Gormley to E. Johnson re: Files	JX 2 see Tr. 6:15-16			
RX369	Email from C. Gormley to E. Johnson re: Medical Insurance Terms	JX 2 see Tr. 6:15-16			
RX370	Johnson/Tiversa Medical Insurance Terms List	JX 2 see Tr. 6:15-16			
RX371	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX372	Email from C. Gormley to E. Johnson re: link	JX 2 see Tr. 6:15-16			
RX373	Email from C. Gormley to E. Johnson re: link	JX 2 see Tr. 6:15-16			
RX374	Email from C. Gormley to E. Johnson re: post-release	JX 2 see Tr. 6:15-16			
RX375	Email from C. Gormley to E. Johnson re: are you..	JX 2 see Tr. 6:15-16			
RX376	Email from C. Gormley to E. Johnson re: fax of the revision should be arriving now	JX 2 see Tr. 6:15-16			
RX377	Email from C. Gormley to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX378	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX379	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX380	Email from C. Gormley to E. Johnson re: Final Example	JX 2 see Tr. 6:15-16			
RX381	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX382	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX383	Email from C. Gormley to E. Johnson re: Healthcare Study	JX 2 see Tr. 6:15-16			
RX384	Email from C. Gormley to E. Johnson re: Link	JX 2 see Tr. 6:15-16			
RX385	Email from C. Gormley to E. Johnson re: pr	JX 2 see Tr. 6:15-16			
RX386	Email from C. Gormley to E. Johnson re: Public Hospital Footpring	JX 2 see Tr. 6:15-16			
RX387	Email from C. Gormley to E. Johnson re: Sending Over Thoughts	JX 2 see Tr. 6:15-16			
RX388	Email from C. Gormley to E. Johnson re: Sending Over Thoughts	JX 2 see Tr. 6:15-16			
RX389	Email from C. Gormley to E. Johnson re:	JX 2 see Tr. 6:15-16			
RX390	Email from E. Johnson to C. Gormley re:	JX 2 see Tr. 6:15-16			
RX391	Email from E. Johnson to C. Gormley re:	JX 2 see Tr. 6:15-16			
RX392	Email from E. Johnson to C. Gormley re: Dartmouth	JX 2 see Tr. 6:15-16			
RX393	Email from E. Johnson to C. Gormley re: Diagnostic Codes	JX 2 see Tr. 6:15-16			
RX394	Email from E. Johnson to C. Gormley re: Final Example	JX 2 see Tr. 6:15-16			
RX395	Email from E. Johnson to C. Gormley re: Medical Insurance Terms	JX 2 see Tr. 6:15-16			
RX396	Email from E. Johnson to C. Gormley re: Paper	JX 2 see Tr. 6:15-16			
RX397	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX398	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX399	Email from E. Johnson to R. Wallace re: Files	JX 2 see Tr. 6:15-16			
RX400	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX401	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX402	Email from R. Wallace to E. Johnson re: files	JX 2 see Tr. 6:15-16			
RX403	E. Johnson emails and article re: data hemorrhaging	JX 2 see Tr. 6:15-16	Johnson, Tr. 783-785		

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX404	E. Johnson grant documents	JX 2 see Tr. 6:15-16	Sherman, Tr. 57; Johnson, Tr. 751-755		
RX405	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX406	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX407	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX408	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX409	LabMD Threat Scan	JX 2 see Tr. 6:15-16	Daugherty, Tr. 1041-1042		
RX410	LabMD Threat Scan	JX 2 see Tr. 6:15-16			
RX411	Communications between J.Parr and TrendMicro re:service	JX 2 see Tr. 6:15-16			
RX412	IT expenditure chart	JX 2 see Tr. 6:15-16			CX0683
RX413	Veritas Server Backup Report	JX 2 see Tr. 6:15-16			
RX414	Packet Filtering Summary	JX 2 see Tr. 6:15-16			
RX415	Kaloustian background check/A. Simmons' resignation	JX 2 see Tr. 6:15-16			
RX416	L. Hudson Termination Notice	JX 2 see Tr. 6:15-16			
RX417	Email: R. Yodaiken to K. Jestes, Subject: Contact with FBI	JX 2 see Tr. 6:15-16			
RX418	Email: L. Riposo VanDruff to K. Jestes, Subject: Courtesy copy of subpoena	JX 2 see Tr. 6:15-16			
RX419	Letter: L. Riposo VanDruff to K. Jestes	JX 2 see Tr. 6:15-16			
RX420	Email: D. Ojeda to ASHEER@ftc.gov	JX 2 see Tr. 6:15-16			
RX421	Email: K. Jestes to D. Ojeda, Subject:	JX 2 see Tr. 6:15-16			
RX422	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: Erick Garcia	JX 2 see Tr. 6:15-16			
RX423	Email: msmith4@ftc.gov to K. Jestes, Subject: File Request - Federal Trade Commission – File Request	JX 2 see Tr. 6:15-16			
RX424	Email: K. Jestes to M. Wood, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX425	Letter: (To: REDACTED) from M. Daugherty (No Subject)	JX 2 see Tr. 6:15-16			
RX426	Email: HELPDESK to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX427	Email: R. Yodaiken to K. Jestes, Subject: General ID theft -related information	JX 2 see Tr. 6:15-16			
RX428	Email: A. Sheer to K. Jestes, Subject: Hi Karina. The package arrived safe and sound - thanks. Alain	JX 2 see Tr. 6:15-16			
RX429	Email: A. Sheer to K. Jestes, Subject: LabMD (Attach: redacted LabMDs Letter(3.27.23).pdf)	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX430	Letter: (To: REDACTED) from M. Daugherty (No Subject)	JX 2 see Tr. 6:15-16			
RX431	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX432	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX433	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX434	Email: A. Sheer to K. Jestes, Subject: More id theft links	JX 2 see Tr. 6:15-16			
RX435	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX436	Email: R. Yodaiken to K. Jestes, Subject: our address	JX 2 see Tr. 6:15-16			
RX437	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX438	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX439	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX440	Email: K. Jestes to A. Sheer, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX441	Email: A. Sheer to K. Jestes, Subject: Erick Garcia	JX 2 see Tr. 6:15-16			
RX442	Email: L. Riposo VanDruff to K. Jestes, Subject: follow up	JX 2 see Tr. 6:15-16			
RX443	Email: A. Sheer to K. Jestes, Subject: Hi Karina. The package arrived safe and sound - thanks. Alain	JX 2 see Tr. 6:15-16			
RX444	Email: R. Yodaiken to K. Jestes, Subject: Hi Karina. When you have a moment, could you send the tracking number? Thanks.	JX 2 see Tr. 6:15-16			
RX445	Email: A. Sheer to K. Jestes, Subject: Hi Karina. Would you have a few minutes to talk with us tomorrow (we're clear all day) o Wednesday (in the afternoon) to catch up? Thanks. Alain	JX 2 see Tr. 6:15-16			
RX446	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX447	Email: K. Jestes to A. Sheer, Subject: LabMD	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX448	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX449	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX450	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX451	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX452	Email: A. Sheer to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX453	Email: K. Jestes to A. Sheer, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX454	Email: A. Sheer to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX455	Email: A. Sheer to K. Jestes, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX456	Email: R. Yodaiken to K. Jestes, Subject: LabMD	JX 2 see Tr. 6:15-16			
RX457	Email: L. Riposo VanDruff to K. Jestes, Subject: location for depo	JX 2 see Tr. 6:15-16			
RX458	Email: L. Riposo VanDruff to K. Jestes, Subject: location for depo	JX 2 see Tr. 6:15-16			
RX459	Email: R. Yodaiken to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX460	Email: A. Sheer to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX461	Email: A. Sheer to K. Jestes, Subject: my first phone call	JX 2 see Tr. 6:15-16			
RX462	Email: K. Jestes to HELPDESK, Subject: LabMD from Sacramento Police	JX 2 see Tr. 6:15-16			
RX463	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX464	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX465	Email: R. Yodaiken to A. Sheer and K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX466	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX467	Email: A. Sheer to K. Jestes, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX468	Email: R. Yodaiken to K. Jestes, Subject: Sac County Courts online	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX469	Email: L. Riposo VanDruff to K. Jestes, Subject: subpoena results	JX 2 see Tr. 6:15-16			
RX470	Email: A. Sheer to K. Jestes, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX471	Email: A. Sheer to K. Jestes, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX472	Email: R. Yodaiken to K. Jestes, Subject: Update	JX 2 see Tr. 6:15-16			
RX473	Email: K. Jestes to R. Yodaiken, Subject: release of evidence	JX 2 see Tr. 6:15-16			
RX474	Email: R. Yodaiken to K. Jestes, Subject: sharing documents	JX 2 see Tr. 6:15-16			
RX475	Template (?) to General Counsel FTC, Subject: Request for Non-public Materials and Certification of Intent to Maintain Confidentiality and to Restrict Use to Law Enforcement Purposes	JX 2 see Tr. 6:15-16			
RX476	Email: A. Sheer to K. Jestes, Subject: Attach: 2013.08.27 Letter to Detective Jestes.PDF	JX 2 see Tr. 6:15-16			
RX477	Letter: A. Sheer to K. Jestes, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX478	Email: A. Sheer to K. Jestes, Subject: (no subject)	JX 2 see Tr. 6:15-16			
RX479	Email: K. Jestes to R. Yodaiken and A. Sheer, Subject: upcoming deposition	JX 2 see Tr. 6:15-16			
RX480	Email: K. Jestes to A. Sheer and R. Yodaiken, Subject: Update	JX 2 see Tr. 6:15-16			
RX481	LabMD Electronics Policy	JX 2 see Tr. 6:15-16			
RX482	Cyprus Master Terms	JX 2 see Tr. 6:15-16			
RX483	Emails between C. Gormley and E. Johnson Re: WSJ article	JX 2 see Tr. 6:15-16	Johnson, Tr. 770-775; 776-777		
RX484	Zhao/Johnson article	JX 2 see Tr. 6:15-16			
RX485	Tiversa press release	JX 2 see Tr. 6:15-16			
RX486	Deposition Transcript of John Boyle	JX 2 see Tr. 6:15-16			CX0704
RX486-A	PUBLIC Deposition Transcript of John Boyle	See OALJ Order dated 7/15/2015			CX0704-
RX487	Deposition Transcript of Brandon Bradley	JX 2 see Tr. 6:15-16			CX0705

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX487-A	PUBLIC Deposition Transcript of Brandon Bradley	See OALJ Order dated 7/15/2015			CX0705-
RX488	Deposition Transcript of Sandra Brown	JX 2 see Tr. 6:15-16			CX0706
RX489	Deposition Transcript of Matt Bureau	JX 2 see Tr. 6:15-16			CX0707
RX490	Deposition Transcript of Lou Carmicheal	JX 2 see Tr. 6:15-16			CX0708
RX491	Deposition Transcript of Mike Daugherty	JX 2 see Tr. 6:15-16			CX0709
RX492	Deposition Transcript of LabMD designee, Mike Daugherty	JX 2 see Tr. 6:15-16			CX0710
RX492-A	PUBLIC Deposition Transcript of LabMD designee, Mike Daugherty	See OALJ Order dated 7/15/2015			CX0710-
RX493	Deposition Transcript of Jeremy Dooley	JX 2 see Tr. 6:15-16			CX0711
RX494	Deposition Transcript of Erick Garcia	JX 2 see Tr. 6:15-16			CX0712
RX495	Deposition Transcript of Kim Gardner	JX 2 see Tr. 6:15-16			CX0713
RX495-A	PUBLIC Deposition Transcript of Kim Gardner	See OALJ Order dated 7/15/2015			CX0713-
RX496	Deposition Transcript of [former LabMD employee]	JX 2 see Tr. 6:15-16			CX0714
RX496-A	PUBLIC Deposition Transcript of [former LabMD employee]	See OALJ Order dated 7/15/2015			CX0714-
RX497	Deposition Transcript of Patricia Gilbreth	JX 2 see Tr. 6:15-16			CX0715
RX497-A	PUBLIC Deposition Transcript of Patricia Gilbreth	See OALJ Order dated 7/15/2015			CX0715-
RX498	Deposition Transcript of Nicotra Harris	JX 2 see Tr. 6:15-16			CX0716
RX499	Deposition Transcript of Patrick Howard	JX 2 see Tr. 6:15-16			CX0717
RX500	Deposition Transcript of Lawrence Hudson	JX 2 see Tr. 6:15-16			CX0718
RX501	Deposition Transcript of Robert Hyer	JX 2 see Tr. 6:15-16			CX0719
RX502	Deposition Transcript of Karina Jestes	JX 2 see Tr. 6:15-16			CX0720
RX503	Deposition Transcript of Eric Johnson	JX 2 see Tr. 6:15-16			CX0721
RX504	Deposition Transcript of Eric Knox	JX 2 see Tr. 6:15-16			CX0722
RX505	Deposition Transcript of David Lapides	JX 2 see Tr. 6:15-16			CX0723

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EXHI CROSS REFEREN
RX505-A	PUBLIC Deposition Transcript of David Lapides	See OALJ Order dated 7/15/2015			CX0723-
RX506	Deposition Transcript of Chris Maire	JX 2 see Tr. 6:15-16			CX0724
RX507	Deposition Transcript of Jeff Martin	JX 2 see Tr. 6:15-16			CX0725
RX507-A	PUBLIC Deposition Transcript of Jeff Martin	See OALJ Order dated 7/15/2015			CX0725-
RX508	Deposition Transcript of Alison Simmons	JX 2 see Tr. 6:15-16			CX0730
RX509	Deposition Transcript of Alison Simmons	JX 2 see Tr. 6:15-16			CX0734
RX510	Deposition Transcript of Curt Kaloustian	JX 2 see Tr. 6:15-16			CX0735
RX511	Deposition Transcript of Jennifer Parr	JX 2 see Tr. 6:15-16			CX0727
RX511-A	PUBLIC Deposition Transcript of Jennifer Parr	See OALJ Order dated 7/15/2015			CX0727-
RX512	Deposition Transcript of Kevin Wilmer	JX 2 see Tr. 6:15-16			CX0732
RX512-A	PUBLIC Deposition Transcript of Kevin Wilmer	JX 2 see Tr. 6:15-16			CX0732-
RX513	Deposition Transcript of LeTonya Randolph	JX 2 see Tr. 6:15-16			CX0728
RX514	Deposition Transcript of Peter Sandrev	JX 2 see Tr. 6:15-16			CX0729
RX515	Deposition Transcript of Ruth Yodaiken	JX 2 see Tr. 6:15-16			
RX516	Deposition Transcript of Randall Jerry Maxey	JX 2 see Tr. 6:15-16			CX0726
RX517	Deposition Transcript of Christopher Gormley	JX 2 see Tr. 6:15-16			CX0872
RX518	Complaint Counsel's Responses to LabMD's First Set of Interrogatories	JX 2 see Tr. 6:15-16			
RX519	Complaint Counsel's Responses to LabMD's Second Set of Interrogatories	JX 2 see Tr. 6:15-16			
RX521	RX3 Yodaiken deposition	JX 2 see Tr. 6:15-16			
RX522	Deposition Transcript of Rick Kam	JX 2 see Tr. 6:15-16			
RX523	Deposition Transcript of James Van Dyke	JX 2 see Tr. 6:15-16			
RX524	Deposition Transcript of Raquel Hill	JX 2 see Tr. 6:15-16			
RX525	Deposition Transcript of Daniel Kaufman	JX 2 see Tr. 6:15-16			
RX526	Complaint Counsel's Amended Responses to LabMD's First Set of Request for Admissions	JX 2 see Tr. 6:15-16			

EXHIBIT NUMBER	EXHIBIT DESCRIPTION	ADMISSION REFERENCE PURSUANT TO 16 CFR 3.26(b)	DISCUSSION REFERENCES PURSUANT TO 16 CFR 3.46(b)	SUMMARY EXHIBITS	CX EX CR REFE
RX527	Deposition Transcript of Karina Jestes II	JX 2 see Tr. 6:15-16			
RX528	Ponemon Survey Report	Tr. 484:19; May 18, 2015 JX0002 Joint Status Report on Exhibits	Kam, Tr. 484-489; 496; 529-531; 533-543; 554; 561-568		
RX529	Javelin Questionairre questions	Tr. 708:13; May 18, 2015 JX0002 Joint Status Report on Exhibits	Van Dyke, Tr. 701-715; 717-734		
RX532	Kaufman Deposition Transcript II	Tr. 1116:03-04; May 18, 2015 JX0002 Joint Status Report on Exhibits	Kaufman, Tr. 1115-1116		
RX533	Adam Fisk Expert Report	Tr. 1135:12-13; May 18, 2015 JX0002 Joint Status Report on Exhibits	Fisk, Tr. 1134-1175; 1179-1195; 1196; 1208; 1210; 1474		
RX541	Deposition Transcript of Robert Boback	See OALJ Order dated 7/1/2014	Tr. 1307		
RX542	June 11, 2014 OGR Letter from Issa to Ramirez	See OALJ Order dated 2/12/2015			
RX543	December 1, 2014 OGR Letter from Issa to Ramirez	See OALJ Order dated 2/12/2015			
RX545	CIGNA - Tiversa Incident Record Form ID #CIG00081	Admitted during Hearing on 5/5/2015 at 1419:6	Wallace, Tr. 1391-1396; 1400; 1411-1419; 1449-1452		
RX546	Tiversa Forensic Investigation Report August 12, 2008 for Ticket #CIG00081	Admitted during Hearing on 5/5/2015 at 1425:25	Wallace, Tr. 1398-1408; 1411-1412; 1417-1422; 1425-1426		
RX549	1718 Insurance Aging File Cover Sheet dated 6/5/07 with Wallace 00000100	Admitted during Hearing on 5/5/2015 at 1423:20	Wallace, Tr. 1409-1412; 1422-1423		
RX644	OGR Committee Report on "Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?"	See OALJ Order dated 7/15/2015			
RX645	LabMD Patient Forms/ LabMD Employee Handbook/Auditing guidelines/Insurance Documents and Payment information	See OALJ Order dated 6/22/2015	Tr. 1474-1475		
RX646	RX-15 exhibit to the Yodaiken deposition	See OALJ Order dated 6/22/2015	Tr. 1475-1476		
RX650	Nondisclosure Motion in ND GA Gormley RX-2	See OALJ Order dated 6/22/2015	Tr. 1475-1476		
RX652	Confidentiality Agreement Tiversa / Johnson RX-9	See OALJ Order dated 6/22/2015	Tr. 1475-1476		

RX657	Sales Rep. Agreement (RX-1 Hudson)	See OALJ Order dated 6/22/2015	Tr. 1475-1476		

ATTACHMENT 2

IN THE MATTER OF
LABMD, INC
DOCKET NO. 9357

RESPONDENT COUNSEL'S WITNESS INDEX

NAME	BRIEF IDENTIFICATION	TRANSCRIPT REFERENCES	*IN CAMERA* STATUS
Eric Johnson	Dean of the Business School, Vanderbilt University; Former Director, Tuck Center for Digital Strategies at Dartmouth College	Tr. 749-806	Not *In Camera*
Michael Daugherty	Founder and CEO, LabMD	Tr. 936-1099	Not *In Camera*
Daniel Kaufman	Deputy Director, FTC Bureau of Consumer Protection	Tr. 1100-1117	Not *In Camera*
Adam Fisk	President and CEO, Brave New Software Project	Tr. 1123-1215	Not *In Camera*
Richard Wallace	Forensic Analyst, Tiversa	Tr. 1261-1307; 1320-1467	Not *In Camera*

Notice of Electronic Service

I hereby certify that on August 11, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Proposed Findings of Fact, with:

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

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

I hereby certify that on August 11, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s CORRECTED Proposed Findings of Fact, upon:

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

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

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

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

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

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

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

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

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

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

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

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

Patrick Massari
Attorney