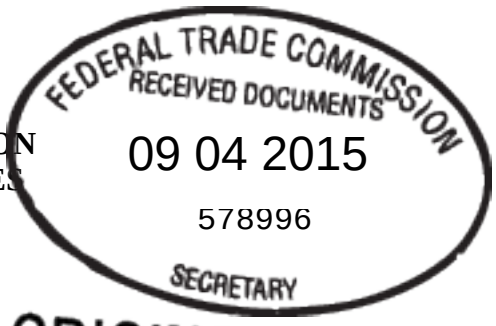
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES



ORIGINAL

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

COMPLAINT COUNSEL'S REPLY TO
RESPONDENT'S PROPOSED FINDINGS OF FACT

Alain Sheer
Laura Riposo VanDruff
Jarad Brown
Ryan Mehm
Megan Cox

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

Complaint Counsel

TABLE OF CONTENTS[1]

[1] In accordance with the Court's Order on Post-Trial Briefs, Complaint Counsel has replicated Respondent's headings to aid the reader.

REFERENCE ABBREVIATIONS

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

Respondent, LabMD, Inc. – Respondent or LabMD

CCFF – Complaint Counsel's Proposed Findings of Fact

CCCL – Complaint Counsel's Proposed Conclusions of Law

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

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

RFF – Respondent's Proposed Findings of Fact

RCL – Respondent's Proposed Conclusions of Law

A. Background

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

Response to Finding No. 1:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. As this Court noted, "[o]nce the Commission has . . . issued a complaint, the issue to be litigated is not the adequacy of the Commission's pre-complaint information or the diligence of its study of the material in question but whether the alleged violation has in fact occurred." Order on Compl. Counsel's Mot. to Quash Subpoena Served on Compl. Counsel and for Prot. Order at 5-6 (Jan. 30, 2014) (quoting *In re Exxon Corp.*, 83 F.T.C. 1759, 1974 FTC LEXIS 226, at *2-3 (1974)); *see also* Order Denying Resp't's Mot. for a Rule 3.36 Subpoena at 4-5 (Feb. 21, 2014); Order Granting Compl. Counsel's Mot. to Quash and to Limit Dep. Subpoenas Served on Comm'n Att'ys at 2-7 (Feb. 25, 2014); Order Granting in Part and Denying in Part Compl. Counsel's Mot. for Prot. Order Regarding Rule 3.33 Notice of Dep. at 3-4 (March 10, 2014). Accordingly, information relating the Commission's pre-complaint investigation and decision to file a complaint are outside the purview of this administrative proceeding.

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)).

Response to Finding No. 2:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1). Furthermore, to the

extent it asserts that the Commission's Complaint was based only on information from the Privacy Institute, the proposed finding is misleading. The Commission issued the Complaint based on extensive evidence it had at the time of LabMD's data security practices, demonstrating LabMD's systemic failure to provide reasonable security for sensitive personal information on its computer networks, and evidence – including documents and testimony from LabMD – that the 1718 File was available for sharing through LimeWire installed on a LabMD computer.

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.").

Response to Finding No. 3[2]:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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

[2] In Proposed Findings Nos. 3, 37-40, 70a, and 71a, Respondent cites to RX541, certain portions of which were accorded *in camera* treatment by the Court's July 1, 2014 Order. A public version of RX541 appears at RX541-A.

sometimes there would be communication that was quite frequent, other times, you know, maybe weekly."); (RX644 [Respondent's Footnote 1 omitted] (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).

Response to Finding No. 4:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses or proposed relief before this Court. (CCRRFF ¶ 1).

To the extent the proposed finding is purportedly supported by RX644, the proposed finding is in violation of the Court's Order on Post-Trial Briefs because the proposed finding cites evidence admitted not for the truth of the matter asserted to support a factual proposition. Order on Resp't's Mot. to Admit Exs. at 3 (July 15, 2015) (admitting RX644 for limited purposes, and not for "the truth of the matters asserted" in statements by Mr. Boback or documents reflected in RX644).

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).

Response to Finding No. 5:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

6. In this press release, 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 "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).

Response to Finding No. 6:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 7:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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).

Response to Finding No. 8:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

To the extent the proposed finding relies on Mr. Shields, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because it cites an opinion by Respondent's expert to support factual propositions that should be established by fact witnesses or documents.

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."

Response to Finding No. 9:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

To the extent the proposed finding is attempting to state a proposition of law, 42 U.S.C. § 1320d-6 was not violated in connection with Complaint Counsel's investigation or prosecution of this case. (CCRRCL ¶¶ 122-125).

Otherwise, to the extent the proposed finding is a quotation of the statute, Complaint Counsel has no specific response.

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*.").

Response to Finding No. 10:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶¶ 1, 9; *see also* CCRRCL ¶¶ 122-125 (42 U.S.C. § 1320d-6 was not violated in connection with Complaint

Counsel's investigation or prosecution of this case). In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

10a. 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)).

Response to Finding No. 10a[3]:

The Relevant Time Period refers to the time period during which Dr. Hill examined LabMD's data security practices, from January 2005 through July 2010. (CX0740 (Hill Report) ¶ 4). The Relevant Time Period merely delimits the opinions of Dr. Hill; it does not cabin Complaint Counsel's allegations or evidence in support of its proposed relief. (Final Prehearing Conf., Tr. 44-46; Order Memorializing Bench Ruling (May 16, 2014)).

Furthermore, the evidence shows that LabMD's unreasonable data security practices continued past July 2010. For instance, LabMD's Policy Manual memorializing its 2010 security practices was missing key elements regarding specific policies on the protection of Personal Information in transit, encryption of stored information, and passwords. (CCFF ¶¶ 452-455). Sandra Brown used her insecure LabMD credentials, "sbrown" and "labmd," to access LabMD's network remotely until 2013. (CX0706 (Brown, Dep. at 10-11, 13)). The Policy Manual requires that backups of highly sensitive Personal Information be stored on employee desktop computers, such as the finance/billing manager's computer. (CX0007 (LabMD

[3] Respondent has reused finding numbers a number of times in its proposed findings of fact. Finding 10 is the first to be re-used (*see* RFF ¶ 10, on pages 6 and 7 of Respondent's Proposed Findings of Fact). For clarity in responding, Complaint Counsel has appended a letter to each of Respondent's subsequent uses of the same finding number throughout its reply (*e.g.*, "10a").

Computer Hardware, Software and Data Usage and Security Policy Manual) at 14-15 (stating policy of saving copy of Lytec Billing System backup on employee computer)). Backups should be isolated because an employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, unauthorized changes, and other threats. (Hill, Tr. 196-97; CX0740 (Hill Report) ¶ 104(b)). Further, LabMD failed to implement the policies it did have, such as by not providing employees with encryption tools to implement the Policy Manual's recommendation that employees encrypt emails containing sensitive information. (CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 7-8; CX0713-A (Gardner, Dep. at 62) (employed November 2010 through December 27, 2013); CCFF ¶ 315; CX0709 (Daugherty, Dep. at 116-18)). Likewise, a ProviDyn scan conducted September 3, 2010 revealed that vulnerabilities were present on LabMD's network. (CCFF ¶ 757 (port 21 open, providing access to Microsoft FTP program running on Mapper server), ¶¶ 792-797 (FTP Supports Clear Text Authentication vulnerability, which made usernames and passwords for the FTP application on Mapper vulnerable to sniffing by transmitting them in clear text, present on Mapper server)). In addition, the evidence shows that Personal Information is currently stored unsecured. (CX0713-A (Gardner, Dep. at 45-46) (paper records and patient specimens moved to Mr. Daugherty's residence; some items stored in a garage that was not always locked, and garage door was found up when Mr. Daugherty was not home); CCCL ¶¶ 66-69). Finally, LabMD has no intention of dissolving as a Georgia corporation, retains the personal information of over 750,000 consumers, and intends to employ the same unreasonable policies and procedures to Personal Information in its possession as it employed in the past. CCCL ¶¶ 60-64.

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.").

Response to Finding No. 11:

The complaint alleges that LabMD failed to provide reasonable security for Personal Information on its computer network "[a]t all relevant times." (Compl. ¶ 10). Furthermore, Complaint Counsel identified in its interrogatory responses that, subject to any evidence introduced after that date, the time frame in which LabMD's data security practices were not reasonable is "January 1, 2005 through the close of evidence at the Hearing in the above-captioned matter." (RX518 (Compl. Counsel's Resps. to LabMD's 1st Set of Interrogs.) at 16, Resp. to Interrog. 22; *see also* CCRRFF ¶ 10a (identifying ongoing unreasonable security practices beyond July 2010)).

B. LabMD

12. LabMD is a small, medical services company providing uro-pathology cancer detection services to physician customers. (Daugherty, Tr. 952).

Response to Finding No. 12:

Complaint Counsel has no specific response.

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

Response to Finding No. 13:

Complaint Counsel has no specific response.

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

Response to Finding No. 14:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 15:

Complaint Counsel has no specific response.

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).

Response to Finding No. 16:

Complaint Counsel has no specific response.

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).

Response to Finding No. 17:

Complaint Counsel has no specific response.

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).

Response to Finding No. 18:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 19:

Complaint Counsel has no specific response.

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

Response to Finding No. 20:

The proposed finding is misleading to the extent that it suggests that it describes LabMD's operations from January 2005 through the close of evidence in this case. Mr. Hyer first worked for LabMD in June 2009 and last provided services to LabMD in March 2012. (CX0719 (Hyer, Dep. at 15-16, 30-33, 46-47, 49)). The Court should disregard the proposed finding to the extent it attempts to describe LabMD's system during time periods outside Mr. Hyer's personal knowledge of its operation.

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).

Response to Finding No. 21:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's process in relation to pre-existing or competing processes and the Court should disregard it as impermissible expert opinion.

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

Response to Finding No. 22:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's

process in relation to pre-existing or competing processes and the Court should disregard it as impermissible expert opinion.

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.").

Response to Finding No. 23:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact.

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).

Response to Finding No. 24:

To the extent the proposed finding relies on RXD04, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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

Response to Finding No. 25:

To the extent the proposed finding suggests that any other laboratory required 12 hours to process tissue samples, the Court should disregard the proposed finding. The cited testimony does not identify any process, system, or business model in which processing time is 12 hours. Furthermore, the cited testimony does not describe the efficiency of LabMD's process in relation

to pre-existing or competing processes and the Court should disregard it as impermissible expert testimony.

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).

Response to Finding No. 26:

To the extent the proposed finding relies on RXD06, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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

Response to Finding No. 27:

To the extent the proposed finding relies on RXD07, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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).

Response to Finding No. 28:

To the extent the proposed finding relies on RXD08, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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.").

Response to Finding No. 29:

To the extent the proposed finding relies on RXD10, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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.").

Response to Finding No. 30:

To the extent the proposed finding relies on RXD11, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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).

Response to Finding No. 31:

To the extent the proposed finding relies on RXD12, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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).

Response to Finding No. 32:

To the extent the proposed finding relies on RXD14, the proposed finding is unsupported and in violation of the Court's Order on Post-Trial Briefs because the evidence cited is a demonstrative exhibit and not substantive evidence. Otherwise, Complaint Counsel has no specific response.

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

Response to Finding No. 33:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 34:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's coding and numbering system in relation to pre-existing or competing coding and numbering systems and the Court should disregard it as impermissible expert testimony.

C. The Origins of FTC's Investigation of LabMD

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).

Response to Finding No. 35:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 36:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 37:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 38:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 39:

The Court should disregard the proposed finding because it is not supported by the citations to the record. CX0541, which Respondent cites, is not part of the evidentiary record. (Compl. Counsel's Witness and Exhibit Indices, Exhibit Index at 19 (Aug. 10, 2015) (noting CX0540 – CX0543 intentionally not used). RX541-A, the June 2014 deposition of Mr. Boback

pursuant to a notice of deposition served by Respondent's Counsel, does not support the proposed finding. In addition, the Court should disregard Respondent's citation to motions practice, which is not part of the evidentiary record. Should the Court consider the proposed finding, Complaint Counsel has no specific response to the extent that it relates to the FBI. In addition, the proposition that Tiversa received direct payment for services to the Department of Transportation is not supported by the evidentiary record.

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)).

Response to Finding No. 40:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and Complaint Counsel's opposition to a motion is not a document in evidence. Furthermore, the opening statement of counsel, to which Respondent refers but fails to cite, is not part of the evidentiary record.

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)).

Response to Finding No. 41:

The proposed finding is irrelevant. Complaint Counsel's choice not to develop testimony that is irrelevant to this matter is not evidence.

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)).

Response to Finding No. 42:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Mr. Boback's hearsay characterization of the Commission's testimony is not accurate to the underlying testimony, and the remaining citation is to a document not in evidence, but is being used to establish a factual proposition, in violation of the Court's Order on Post-Trial Briefs. To the extent the proposed finding characterizes the cited testimony, it is misleading. The Commission's 2007 written statement to the House Committee on Oversight and Government Reform *noted that a 2005 staff report had described P2P software* as a "neutral technology," meaning that the technology itself could be used safely but that user behavior could create risk. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3). The Commission's statement also explained that P2P technology created the risk that users "may unintentionally share personal or other sensitive files residing on their hard drives." (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 2). In addition, the statement set forth the steps that the Commission had taken to warn consumers and businesses of the dangers of P2P file sharing as early as July 2003. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 8-11).

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).

Response to Finding No. 43:

The proposed finding is misleading.[4] Complaint Counsel has no specific response to the second and third bullet points in this finding. The first bullet point, however, uses out-of-context quotes from the Commission's 2007 written statement to the House Committee on Oversight and Government Reform Committee to create several misleading impressions. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3).[5] While the written statement did explain that a 2005 staff report had described P2P software as a "neutral technology," this does not mean it testified that P2P presented no risk. Instead, it explained that the technology itself could be used safely but that user behavior could create risk. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3). The Commission's statement also explained that P2P technology created the risk that users "may unintentionally share personal or other sensitive files residing on their hard drives." (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 2). The statement also set forth the steps that the Commission had taken to warn consumers and

[4] Respondent cites to the testimony of Mary Engle without reference to a document in evidence. However, because the testimony is in evidence as CX0787, Complaint Counsel has not objected on that basis.

[5] The proposed finding relies on a citation to Mary Engle's oral testimony before the Committee. Ms. Engle's testimony does not include the quotations included here.

businesses of the dangers of P2P file sharing as early as July 2003. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 8-11).

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).

Response to Finding No. 44:

The proposed finding is incorrect. The Commission issued warnings concerning the risks of P2P software as early as July 2003. (*See* CCFF ¶¶ 1338-1351).

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)).

Response to Finding No. 45:

The proposed finding is incorrect.[6] The Commission issued warnings concerning the risks of P2P software as early as July 2003. (*See* CCFF ¶¶ 1338-1351). The Commission's 2007 written statement to Congress cannot be read as affirming the use of P2P file sharing. (CX0787

[6] Respondent cites to the testimony of Mary Engle without reference to a document in evidence. However, because the testimony is in evidence as CX0787, Complaint Counsel has not objected on that basis.

(Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3). While the written statement did explain that a 2005 staff report had described P2P software as a "neutral technology," this does not mean it testified that P2P presented no risk. Instead, it explained that the technology itself could be used safely but that user behavior could create risk. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3). The Commission's statement also explained that P2P technology created the risk that users "may unintentionally share personal or other sensitive files residing on their hard drives." (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 2). The statement also set forth the steps that the Commission had taken to warn consumers and businesses of the dangers of P2P file sharing as early as July 2003. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 8-11). At most the statement indicated that there might be possible legitimate uses for P2P sharing technology for businesses where steps had been taken to reduce the risk of user error. LabMD's use of LimeWire was not such a use. (*See* CCFF ¶¶ 1363-1390).

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.").

Response to Finding No. 46:

The Court should disregard the proposed finding because it is not supported by the citation to the record.[7] The cited document states that the Commission encouraged improved practices and self-regulation. (*See* CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report) at 26). ("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."). There is no evidence in the record to support a finding that the Commission "worked with" P2P software providers.

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)).

Response to Finding No. 47:

The Court should disregard the proposed finding because it cites to a document that is not in evidence in violation of the Court's Order on Post-Trial Briefs. Furthermore, the proposed finding is not supported by its citation, and is incorrect. The Commission issued warning concerning the risks of P2P software as early as July 2003. (*See* CCFF ¶¶ 1338-1351).

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

Response to Finding No. 48:

Complaint Counsel has no specific response.

[7] Respondent cites to a Commission staff report without reference to a document in evidence. However, because the document is in evidence as CX0777, Complaint Counsel has not objected on that basis.

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).

Response to Finding No. 49:

To the extent that the proposed finding states that Mr. Wallace testified that when he was first working for Tiversa, he was instructed to find information relevant to a congressional hearing, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record.

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).

Response to Finding No. 50:

To the extent that the proposed finding states that Mr. Wallace testified that Mr. Boback's statement to Congress in 2007 that Tiversa's system had downloaded certain documents was not true, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 49a:

Complaint Counsel has no specific response.

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

Response to Finding No. 50a:

To the extent that the proposed finding states that Mr. Wallace testified that Tiversa would scour peer-to-peer networks and download information available on predominantly the Gnutella network, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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).

Response to Finding No. 52:

The proposed finding is misleading because it omits the context of Mr. Wallace's statement. In the testimony cited by Respondent, Mr. Wallace described efforts to prepare for a congressional hearing. To the extent that the proposed finding states that Mr. Wallace testified that, in preparing for a congressional hearing, Mr. Wallace was instructed to "use any and all means available to find information that would be relevant for that hearing. . . . Everything from health insurance information to [] PII, Social Security numbers, basically anything that should not be out [] on these networks" (Wallace, Tr. 1341), Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding.

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).

Response to Finding No. 51:

Complaint Counsel has no specific response.

52a. 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)).

Response to Finding No. 52a:

The Court should disregard the proposed finding because it cites to a document containing hearsay statements that are not in the evidentiary record. Moreover, the URL provided in Respondent's proposed finding links only to Mr. Boback's oral statement, contrary to Respondent's citation.

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.").

Response to Finding No. 53:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 54:

To the extent that the proposed finding states that Mr. Wallace would search and download files from the P2P networks using off-the-shelf peer-to-peer clients, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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.").

Response to Finding No. 55:

Complaint Counsel has no specific response.

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).

Response to Finding No. 56:

The proposed finding is misleading in its references to "potential targeted entities," "existing clients," and "fraudulent 'spread' or proliferation" subjects that are not addressed by Mr. Wallace's testimony at Respondent's citations to the evidentiary record. To the extent that the proposed finding states that Mr. Wallace testified that when he downloaded a "significant" file from the peer-to-peer network, he would "go to [Mr. Boback] . . . and [Mr. Boback] would make the decision" whether to give the information to a salesperson or call the company directly in an effort to monetize the information, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the cited evidentiary record.

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).

Response to Finding No. 57:

The proposed finding is misleading to the extent that it contends that the cited evidence establishes that Mr. Wallace recorded the "type of file" or that he recorded any information when he "downloaded or 'pulled down'" files from P2P networks. Rather the cited evidence relates to the information Mr. Wallace viewed and recorded when he was "viewing files." (Wallace, Tr. 1344-1345). Accordingly, the Court should disregard the proposed finding.

49b. 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).

Response to Finding No. 49b:

To the extent that the proposed finding states that on or about February 25, 2008, Rick Wallace downloaded a LabMD insurance aging file that was 1,718 pages in length from a LabMD computer, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

50b. 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).

Response to Finding No. 50b:

The Court should disregard the proposed finding because it is misleading and improperly presented as proposed finding of fact. First, there is no evidence in the record regarding purported "victims" of the activity described in the proposed finding. To the extent that any individual or entity may have been "victimized" by the activity described in the proposed finding, such a characterization constitutes a legal conclusion, not a fact. That legal conclusion

is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs. Second, Respondent's contention regarding Mr. Wallace's skills constitute an opinion that is not supported by any expert testimony. Nor do the citations to the evidentiary record support Respondent's contention regarding Mr. Wallace's skills. The remaining contentions of the proposed finding are not supported by the cited evidentiary record.

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

Response to Finding No. 51a:

To the extent that the proposed finding states that Mr. Wallace at one time worked with law enforcement, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record.

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

Response to Finding No. 52b:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Specifically, even if Mr. Wallace were competent to establish Mr. Boback's intent in hiring Mr. Wallace, none of Respondent's citations relate to Mr. Boback's intention in that regard.

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

Response to Finding No. 53a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. That legal conclusion is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs. Furthermore, the Court should disregard the proposed finding because it is not supported by the citation to the record.

54a. 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).

Response to Finding No. 54a:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

55a. 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).

Response to Finding No. 55a:

To the extent that the proposed finding states that Mr. Wallace testified that he created the illusion that companies' data had proliferated on peer-to-peer networks, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by Respondent's citation to the evidentiary record.

56a. 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).

Response to Finding No. 56a:

The Court should disregard entirely the proposed finding because it attempts to state a legal conclusion, not a fact. That legal conclusion is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs. If the Court nonetheless considers the proposed finding, to the extent that the proposed finding states that Mr. Wallace testified that he created CX0019, following a discussion with Mr. Boback, to make it appear as if LabMD's insurance aging file had not come from an IP address in the Atlanta area, Complaint Counsel has no specific response. The remaining contentions of the proposed finding are not supported by the citation to the record.

57a. 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).

Response to Finding No. 57a:

To the extent that the proposed finding states that Mr. Wallace testified that he created the list of IP addresses contained in CX0019 following a conversation with Mr. Boback, that those IP addresses were of information concentrators known to Mr. Wallace, and that Mr. Wallace placed the information contained in CX0019 in Tiversa's data store, Complaint Counsel has no specific response. The remaining contentions of the proposed finding include legal conclusions that are not facts, and they are not supported by the citation to the record. Those

legal conclusions are unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs.

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).

Response to Finding No. 58:

To the extent that the proposed finding states that Mr. Wallace testified that he, Mr. Boback, and Commission staff met to discuss information that had been produced to the Commission pursuant to a CID, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it is not supported by the citation to te record, and is misleading. First, the proposed finding deliberately suggests that Commission staff participated in a meeting or discussion with Mr. Wallace or Mr. Boback that related to falsifying evidence or "mak[ing] it appear that LabMD's insurance aging file had spread on P2P networks." Since this scurrilous suggestion is not supported by the cited testimony or any other evidence, and is in fact contradicted by the cited testimony, the court should disregard the proposed finding. Second, contrary to the testimony cited, the proposed finding states that Mr. Wallace and Mr. Boback met with FTC officials "with a view towards" creating a false

document. In fact, Mr. Wallace testified that he and Mr. Boback did not discuss creating a false document until after the meeting ("Bob spoke to me about next steps on the way home."), demonstrating that the proposed finding's characterization of the purpose of the meeting is inaccurate.

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)).

Response to Finding No. 59:

The Court should disregard the proposed finding because it is not supported by the citations to the record. To the contrary, there is no testimony in the record regarding the genesis of "the Commission's interest in LabMD" because the decision-making process of the agency in this regard is not relevant to the claims, defenses, or proposed relief in this matter. *See* Order on Compl. Counsel's Mot. to Quash Subpoena Served on Compl. Counsel and for Prot. Order at 5-6 (Jan. 30, 2014) (citing *Exxon Corp.*, Docket No. 8934, 83 F.T.C. 1759, 1974 FTC LEXIS 226, at *2-3 (1974)). *See also* Order Denying Resp't's Mot. for a Rule 3.36 Subpoena at 4-5 (Feb. 21, 2014); Order Granting Compl. Counsel's Mot. to Quash and to Limit Dep. Subpoenas Served on Comm'n Att'ys at 2-7 (Feb. 25, 2014); Order Granting in Part and Den.ying in Part Compl. Counsel's Mot. for Prot. Order Regarding Rule 3.33 Notice of Dep. at 4 (March 10, 2014).

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).

Response to Finding No. 60:

To the extent that the proposed finding states that Commission staff contacted Professor Eric Johnson to request a copy of a new article concerning health information available on P2P

networks, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record.

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)).

Response to Finding No. 61:

The Court should disregard the proposed finding because it is not supported by the citations to the record. In addition, Dr. Hill's deposition testimony does not relate in any way to Dr. Johnson's "work," as suggested by Respondent's citation to RX524. Finally, the proposed finding improperly cites the testimony of a lay witness for an expert opinion. (*See, e.g.*, Order Granting Mot. in Limine to Limit the Test. of Eric Johnson (May 8, 2014)).

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)).

Response to Finding No. 62:

The proposed finding is misleading to the extent that it suggests that Tiversa received any federal funds in connection with research performed by Dartmouth College and Dr. Johnson. (*Cf.* CX0721 (Johnson, Dep. at 80-82); Johnson, Tr. 773). In addition, the proposed finding is supported by neither the citation to Mr. Daugherty's trial testimony nor the opening statement of counsel, which is not part of the evidentiary record.

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)).

Response to Finding No. 63:

The Court should disregard the proposed finding because it is not supported by the citations to the record. In addition, the Court should disregard the proposed finding to the extent

that it attempts to state a legal conclusion regarding the property interests of health care providers in certain information. That legal conclusion is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs.

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).

Response to Finding No. 64:

The Court should disregard the proposed finding because it is irrelevant and calls for a legal conclusion. In addition, the Court should disregard the proposed finding to the extent that it characterizes legal obligations created by HIPAA. (CCRRCL ¶¶ 122-125).

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)).

Response to Finding No. 65:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 66:

The Court should disregard the proposed finding because it is not supported by the citations to the record. The cited testimony contradicts Respondent's contention that Dartmouth did not obtain the 1718 File using its search terms combined with Tiversa's technology. (*Cf.* Johnson, Tr. 776-777 ("I know that we didn't find it in phase one and that it was found as part of our learning process with Tiversa during this time."); CX0872 (Gormley, Dep. at 100) ("Q.

Would you agree that what he's asking for . . . is information that Tiversa found outside of the Dartmouth digital signature? A. Not necessarily.")).

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)).

Response to Finding No. 67:

The Court should disregard the proposed finding to the extent that it states Tiversa had concluded searching using Dartmouth's search terms in April 2008 because that contention is not supported by the citations to the record.

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)).

Response to Finding No. 68:

The Court should disregard the proposed finding because it is not supported by the citations to the record.

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)).

Response to Finding No. 69:

The Court should disregard the proposed finding because it is not supported by the citation to the record. In addition, the Court should disregard the proposed finding to the extent that it characterizes legal obligations created by HIPAA. (CCRRCL ¶¶ 122-125). In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

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)).

Response to Finding No. 70:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 71:

To the extent that the proposed finding states that LabMD instructed Tiversa to direct further communications to LabMD's lawyer, Complaint Counsel has no specific response.

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)).

Response to Finding No. 72:

The proposed finding is misleading. To the extent that the proposed finding states that the former Chairman of the United States House Oversight and Government Reform Committee initiated an investigation of the activities of Tiversa, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it violates the Court's February 12, 2015 Order on Respondent's Motion to Admit Proffered Exhibits RX542-RX548 and the Court's Order on Post-Trial Briefs. *See* Order on Resp't's Mot. to Admit Proffered Exs. RX 542-RX548 (Feb. 12, 2015) ("February 12, 2015 Order"). Specifically, in ruling on Respondent's Motion to Admit Proffered Exhibits RX542-RX548, the Court held that

it would take official notice or judicial notice only of certain facts. February 12, 2015 Order at 3. The facts of which the Court took notice did *not* include Respondent's contention that OGR was "exploring FTC's relationship with Tiversa." The Court's July 15, 2015 Order on Respondent's Motion to Admit Exhibits, to which the proposed finding does not cite, also provides no support for Respondent's contention that OGR was "exploring FTC's relationship with Tiversa." *See* Order on Resp't's Mot. to Admit Exs. (July 15, 2015).

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)).

Response to Finding No. 73:

The Court should disregard the proposed finding because it expressly contravenes the Court's July 15, 2015 Order on Respondent's Motion to Admit Exhibits, which denied Respondent's Motion to admit RX644, subject to certain limitations unrelated to Respondent's proposed finding. *See* Order on Resp't's Mot. to Admit Exs. (July 15, 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)).
- 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)).

Response to Finding No. 74:

The Court should disregard the proposed finding because it expressly violates the Court's July 15, 2015 Order on Respondent's Motion to Admit Exhibits, which, *inter alia*, permitted the admission of RX644 *not* for the truth of the matters asserted therein and subject to certain limitations unrelated to Respondent's proposed finding. Each of the bulleted "claims" identified by Respondent's proposed finding are thus unsupported by the evidentiary record. *See* Order on Resp't's Mot. to Admit Exhibits at 3 (July 15, 2015). To the extent this finding is meant to show only that the report reached these conclusions but not to show that they are true, the finding is irrelevant to any claim or defense in this proceeding. The contents of former Chairman Issa's report have no bearing on this case.

To the extent that the proposed finding states that Wallace testified that Tiversa communicated with Commission staff in 2007, and that Mr. Wallace testified to having met with FTC staff in 2009, Complaint Counsel has no specific response. The remaining contentions of the proposed finding are unsupported by Respondent's citations to specified portions of Mr. Wallace's testimony. In particular, the testimony Respondent excerpts on pages 25 and 26 of its Proposed Findings of Fact, in support of the contention that "Wallace testified to a meeting in August 2009 between Tiversa and FTC that led Boback to demand evidence of 'spread,'" was admitted for a purpose other than for the truth of the matter asserted. (Wallace, Tr. 1386-1388).

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)).

Response to Finding No. 75:

The Court should disregard the proposed finding because Commissioner Rosch's dissenting statement from the Commission's vote affirming Commissioner Brill's letter decision denying Respondent's and Mr. Daugherty's Petitions to Limit or Quash does not constitute evidence of any fact relevant to the claims, defenses, or proposed relief in this matter. The Court should also disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

72a. 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).

Response to Finding No. 72a:

The proposed finding is misleading in its characterization of the frequency of meetings between FTC staff and Tiversa staff, which is not supported by the citation to the record. Complaint Counsel agrees that Respondent's citation to the evidentiary record supports the contention that FTC staff met with Tiversa staff at Tiversa's headquarters in Pennsylvania. To the extent that the proposed finding states that Mary Engle serves or served as a Commissioner of the Federal Trade Commission, that contention is not supported by the evidentiary record.

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

Response to Finding No. 73a:

To the extent that the proposed finding states that FTC staff travelled to Tiversa's offices in Pennsylvania, Complaint Counsel has no specific response. The Court should otherwise

disregard the proposed finding because the citation to the evidentiary record does not support the contention that the purpose of the travel was to "get a demonstration of the technology."

74a. 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).

Response to Finding No. 74a:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Wallace testified that he did not know who determined the threshold. (Wallace, Tr. 1362 ("Q. And who determined that threshold? A. I am not sure. I know it came – I received the threshold from Bob Boback.")).

75a. 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)).

Response to Finding No. 75a:

The proposed finding is misleading to the extent that it characterizes there having been an "agree[ment]" between the Commission and Tiversa or that such an agreement was for the purpose of "funnel[ing] information from Tiversa to FTC." The cited testimony states that there was a request from Tiversa that Commission staff issue a CID to the Privacy Institute, and the Privacy Institute received the CID from the Commission. (RX525 (Kaufman, Dep. at 20)). The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 76:

The proposed finding is misleading because it is ambiguous what Respondent refers to by "to accomplish this." Mr. Boback testified that Tiversa's counsel formed the Privacy Institute.

(CX0703 (Boback, Dep. at 38-40)). The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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).

Response to Finding No. 77:

To the extent that the proposed finding states that Mr. Wallace testified that he collected information to be provided in response to the CID that the FTC served on the Privacy Institute, Complain Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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).

Response to Finding No. 78:

The proposed finding is misleading because it is ambiguous what Respondent refers to as "[t]he list Wallace provided." In addition, the proposed finding is misleading because the citation to the evidentiary record does not support the contention that Mr. Wallace provided any list. To the extent that the proposed finding states that Mr. Wallace testified that a document produced in response to the CID that the FTC served on the Privacy Institute began from a working copy of Tiversa's incident response case spreadsheet, Complaint Counsel has no specific response. In addition, to the extent that the proposed finding states that Mr. Wallace testified that Tiversa salespeople and Mr. Boback would use information contained on the incident response case spreadsheet to offer remediation services to certain companies, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record.

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).

Response to Finding No. 79:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

69a. 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)).

Response to Finding No. 69a:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

70a. 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)).

Response to Finding No. 70a:

The Court should disregard the proposed finding because it is not supported by the citation to the record. CX0541, which Respondent cites, is not part of the evidentiary record. (Compl. Counsel's Witness and Exhibit Indices, Exhibit Index at 19 (Aug. 10, 2015) (noting CX0540 – CX0543 intentionally not used). RX541-A, the June 2014 deposition of Mr. Boback pursuant to a notice of deposition served by Respondent's Counsel, does not support the proposed finding.

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

Response to Finding No. 71a:

The Court should disregard the proposed finding because it is not supported by the citation to the record. CX0541, which Respondent cites, is not part of the evidentiary record.

(Compl. Counsel's Witness and Exhibit Indices, Exhibit Index at 19 (Aug. 10, 2015) (noting CX0540 – CX0543 intentionally not used).

72b. 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).

Response to Finding No. 72b:

To the extent that the proposed finding states that Mr. Wallace testified that he created CX0019 to demonstrate spread of the 1718 File and "move it off of" an Atlanta IP address, Complaint Counsel has no specific response. (Wallace, Tr. 1381). Mr. Wallace's testimony in this regard is contradicted by the testimony of Mr. Boback. (RX541-A (Boback, Dep. at 22-36, 74-80)).

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

Response to Finding No. 73b:

To the extent that the proposed finding states that Mr. Wallace testified that the 1718 File was never found at any of the four IP addresses contained on CX0019, Complaint Counsel has no specific response. Mr. Wallace's testimony in this regard is contradicted by the testimony of Mr. Boback. (RX541-A (Boback, Dep. at 74-80)).

74b. 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).

Response to Finding No. 74b:

To the extent that the proposed finding states that Mr. Wallace testified that when a company refused to do business with Tiversa, the company's information would appear to proliferate in Tiversa's data store, Complaint Counsel has no specific response. In addition, to the extent that the proposed finding states that Mr. Wallace testified that Mr. Boback indicated

that LabMD appeared at the top of a list, Complaint Counsel has no specific response. Mr. Wallace's testimony in this regard is contradicted by the testimony of Mr. Boback. (CX0703 (Boback, Dep. at 120-21)).

75b. 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).

Response to Finding No. 75b:

To the extent that the proposed finding states that Boback testified that Tiversa "responded to the civil investigative demand exactly to the letter," and that Mr. Wallace testified that some of Tiversa's clients were removed from a list Tiversa produced in response to the CID, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record.

76a. 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).

Response to Finding No. 76a:

The Court should disregard the proposed finding because it does not constitute a fact relevant to the claims, defenses, or proposed relief in this matter.[8]

77a. 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)).

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

Response to Finding No. 77a:

The proposed finding is misleading because it suggests that the citations to the record reflect Messrs. Boback and Kaufman's substantive descriptions of 2009 discussions between Commission staff and Tiversa. The citations to the record do not support Respondent's contention in this regard. To the extent that the proposed finding states that in 2009, Commission staff met with Tiversa staff, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record.

78a. 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).

Response to Finding No. 78a:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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

Response to Finding No. 79a:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 80:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 81:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 82:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 83:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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

Response to Finding No. 84:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 85:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1). Furthermore, Respondent's proposed finding is inaccurate. The Commission, not Complaint Counsel, filed a Complaint and Notice Order against LabMD on August 28, 2013.

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)).

Response to Finding No. 86:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 87:

To the extent it purports to states the opinion of Complaint Counsel's expert Dr. Hill, the Court should disregard the proposed finding because it is not supported by the citation to the record. In addition, to the extent it asserts that the allegations of the Complaint are limited to the time period 2005 to July 2010, the Court should disregard the proposed finding because it is not supported by the citation to the record. The Complaint alleges that "at all relevant times," LabMD "failed to provide reasonable and appropriate security for personal information on its computer networks" (Compl. ¶ 10), and that LabMD's "failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information . . . caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers" (Compl. ¶ 22). Complaint Counsel's proofs are not limited to the time period for which Professor Hill provided an opinion. (*See* CCFF ¶ 13; Hill, Tr. 324).

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).

Response to Finding No. 88:

The proposed finding is misleading. Although Dr. Hill testified that she did not rely on FTC guidance, FTC guidance is consistent with Dr. Hill's approach and other data security standards and guidance that Dr. Hill considered, and that are available to companies. (CCRRFF ¶ 340).

Moreover, as the Bureau and the Commission have consistently stated, the test of whether data security practices are unfair under Section 5 is reasonableness. (RX532 (Kaufman, Dep. at 211); Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf) ("The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of the available tools to improve security and reduce vulnerabilities."); CCRRCL ¶ 145). Dr. Hill evaluated LabMD's data security practices under that test (CX0740 (Hill Report) ¶¶ 2, 45), and opined that it failed to provide reasonable security for Personal Information within its computer network. (CX0740 (Hill Report) ¶ 49). Thus she relied on the only relevant test for whether data security practices violate Section 5.

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.").

Response to Finding No. 89:

To the extent the proposed finding states that Dr. Hill did not consider FTC data security standards or guidelines, it is misleading. To the extend Dr. Hill did not rely on FTC data security business guidance, her approach and the other standards and guidelines she considered are consistent with the FTC's data security business guidance publications. (CCRRFF ¶ 340).

Furthermore, Dr. Hill considered the only relevant test of whether data security practices violate Section 5, which is reasonableness. (CCRRFF ¶¶ 88, 333; CCRRCL ¶ 145).

To the extent the proposed finding assets that Dr. Hill did not consider HIPAA guidelines, the Court should disregard it because it is not supported by the citations to the record, is incorrect, and is irrelevant. Dr. Hill testified that she considered the Security Rule promulgated under HIPAA. (Hill, Tr. 231, 246). In addition, Dr. Hill testified that she considered as part of the HIPAA documents HIPAA Security Series 6 - Basics of Risk Analysis and Risk Management, promulgated by HHS (CX0405). (Hill, Tr. 232; CX0740 (Hill Report) at 65). Furthermore, to the extent the proposed finding asserts that Dr. Hill did not consider a different document or guideline, it should be disregarded because "the HIPAA guidelines" is ambiguous. Regardless, the proposed finding is irrelevant because HIPAA is irrelevant to this case. (*See* CCRRFF ¶¶ 298-99).

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)).

Response to Finding No. 90:

The Court should disregard the proposed finding because it is not supported by a citation to the record, in violation of the Court's Order on Post-Trial Briefs. The cited authority is not in the record but is being offered to support a factual proposition. Moreover, the proposed finding is not supported by the citation and is incorrect. The Commission first released "*Protecting Personal Information: A Guide for Business*," containing five basic steps to create an information security program, in March 2007. *See* Press Releases: FTC Unveils Practical Suggestions for Business on Safeguard Personal Information (Mar. 8, 2007), *available at*

https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding. It has updated the guide multiple times since then, as information security evolves.

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)).

Response to Finding No. 92:

To the extent the proposed finding asserts that LabMD's Employee Handbook stated the information above, and that many LabMD employees received the handbook, Complaint Counsel has no specific response. To the extent the proposed finding asserts that LabMD employees were *effectively* informed of the stated content through receiving or reading the Handbook, the proposed finding is contradicted by the weight of the evidence. (CCFF ¶¶ 894-900 (§ 4.5.2.3 LabMD's Written Policies and Documentation Did Not Provide Instruction to Employees on How to Safeguard Personal Information); *see generally* CCFF ¶¶ 852-900 (§ 4.5 LabMD Did Not Adequately Train Employees to Safeguard Personal Information)).

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)).

Response to Finding No. 93:

To the extent the proposed finding paraphrases the text of the Handbook Receipt Acknowledgment, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record and misleading. As to the claim that "each and every employee" signed the form during the Relevant Time, the proposed finding is unsupported because it does not include any reference to the record

of a signed acknowledgement form for every LabMD employee. CX0130 does not include, for example, signed forms from the following people who were employed by LabMD during the Relevant Time Period: Michael Daugherty (CCFF ¶¶ 305-306); Kim Gardner (CCFF ¶¶ 315-317); Lawrence Hudson (CCFF ¶¶ 340-341); and Eric Knox (CCFF ¶¶ 354-355). The proposed finding is also misleading to the extent that it suggests that signed forms were executed when an employee was first hired and therefore covered their entire employment period because it is contradicted by the weight of the evidence. John Boyle, after being hired, discovered that employees at the time had not signed acknowledgment forms at all. (RFF ¶ 213).

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)).

Response to Finding No. 94:

To the extent the proposed finding asserts that the LabMD Employee Handbook included the stated limitations on the use of LabMD computers, Complaint Counsel has no specific response. However, the proposed finding is not supported by a citation to the record to the extent it asserts that all LabMD employees received the Employee Handbook at the start of the tenure at LabMD. (*See* CCRRFF ¶ 93 (Boyle found some employees had not signed acknowledgement of receiving Handbook)).

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)).

Response to Finding No. 95:

To the extent the proposed finding asserts that LabMD had a Compliance Program document that states it is effective January 2003, or that the Compliance Program document

CX0005 sets forth the *only* "Policies and Standards of Conduct" LabMD had in place to comply with "Compliance Protocols, laws, statutes, regulations, rules and guidance under which LabMD operated" for the period 2003–2008, Complaint Counsel has no specific response.

However, to the extent the proposed finding asserts that LabMD's Compliance Program document sets forth *all* "Policies and Standards of Conduct regarding Protocols, laws, statutes, regulations, rules and guidelines" LabMD was required by law to have in place, the proposed finding is *contradicted* by the citation to the record. The Compliance Program document itself proves that it does not set forth all such "Policies and Standards of Conduct." For example, it states "LabMD shall place policies and procedures in place *in addition to the compliance program* to monitor and insure that patient information is secure, kept private and only used for care, billing, or operational uses . . . . (CX0005 (LabMD Compliance Program) at 4) (emphasis added). The Compliance Program acknowledges LabMD's understanding that securing patient information is a legal obligation, stating: "[a]ny use of patient information given to an un [sic] authorized recipient is a violation of Federal Law," (CX0005 (LabMD Compliance Program) at 4). This statement proves LabMD understood that *additional* policies and procedures regarding security and privacy of personal information were required. Nonetheless, no such additional policies and procedures are contained in the Compliance Program document. (CX0005 (LabMD Compliance Program) at 1-10). And the evidentiary record is clear that no additional policies and procedures existed in writing until 2010. (*E.g.*, CCFF ¶¶ 415-417). Nor were any additional procedures disclosed in the Compliance Training LabMD administered to new hires, which like the Compliance Program document only alluded generally to the obligation to protect personal information. (CCFF ¶¶ 872-875). Accordingly, the Compliance Program document itself contradicts the proposed finding.

Second, to the extent the proposed finding asserts that the Compliance Program document sets forth all of the "Compliance Protocols, laws, statutes, regulations, rules and guidelines" with which LabMD was required to comply, the Court should disregard the proposed finding because it attempts to state a legal conclusion, and the proposed legal conclusion is not supported by the citation to the record. To conclude that the Compliance Program document specifies *all* laws and regulations with which LabMD must comply would require consideration of facts not in the record and law irrelevant to this proceeding. In addition, the proposition that the Compliance Program sets forth the laws with which LabMD must comply is not supported by the citation because the Compliance Program document does not specify any *laws* with which it was put in place to comply. (CX0005 (LabMD Compliance Program) at 1-10). LabMD has provided no evidence of any other document that would supplement its "Compliance Program" besides CX0005 and potentially the Compliance Training it provided (s*ee* CX0127 (LabMD Compliance Training PowerPoint Slides)), neither of which supports the proposition.

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)).

Response to Finding No. 96:

The proposed finding is misleading and unsupported, as follows:

Data Backup Policy: To the extent the proposed finding implies that the "Data Backup Policy" was a written policy, it is contradicted by the weight of the evidence. CX0006, including the Data Backup Policy, did not exist in writing until 2010 (CCFF ¶¶ 415-417, 446-448), and thus was not available to guide LabMD employees until 2010. A comprehensive information security program should be in writing to provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes

as threats evolve. (CCFF ¶ 411). Otherwise, Complaint Counsel has no specific response to the proposed finding that LabMD had the Data Backup Policy beginning in 2001.

Employee User Account Policy: To the extent that it claims that the Employee User Account Policy in CX0006 was set out in writing in 2001, the proposed finding is contradicted by the weight of the evidence. The written CX0006, including the Employee User Account Policy which requires employees to have unique user names and passwords, did not exist in writing until 2010 (CCFF ¶¶ 415-417, 446-448), and thus the policy was not available to guide LabMD employees until 2010. The proposed finding is contradicted by the weight of the evidence as to the claim that the policy was "in practice" starting in 2001 (*see* CCFF ¶¶ 926-971), including because of evidence that a number of employees used "labmd" as their password, or shared passwords that could be used to access Personal Information (CCFF ¶¶ 947-951, 957, 962-963, 969-970), violating any "in practice" policy that required unique usernames and passwords (*see* CX0006 (LabMD Policy Manual) at 12). Furthermore, to the extent that the proposed finding implies that LabMD adequately trained or disseminated this "in practice" policy to its employees, the proposed finding is not supported by any reference to the record, and is contradicted by the weight of the evidence. (*See generally* CCFF ¶¶ 903-993 (§ 4.6 LabMD Did Not Require Common Authentication-Related Security Measures)).

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)).

Response to Finding No. 97:

The proposed finding is misleading and unsupported, as follows:

All Policies: To the extent that it suggests that the 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 in CX0006 (LabMD Policy Manual) were set out in writing in 2002, the proposed finding is contradicted by the weight of the evidence. CX0006, including these policies, did not exist in writing until 2010 (CCFF ¶¶ 415-417, 446-448), so none of them were available to guide LabMD employees until 2010. A comprehensive information security program should be in writing to provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes as threats evolve. (CCFF ¶ 411).

Desktop Monitoring Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Desktop Monitoring Policy was "in practice" starting in 2002. The policy on its face required LabMD to routinely review desktop computers to ensure that security measures were working, software was updated, scans were conducted and reviewed, and errors and warnings were addressed. (CX0006 (LabMD Policy Manual) at 11). In fact, LabMD did not regularly update virus definitions on employee computers, conduct or review antivirus scans on the computers, or ensure that the antivirus programs were working correctly (CCFF ¶¶ 527-529, 531-536, 566-609), and its walk-around inspections of employee computers were haphazard and ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696).

Document Backup Software Policy: Complaint Counsel has no specific response to the proposed finding that the Document Backup Software Policy required employees to save business documents, including documents that may contain Personal Information, to servers and

in the "My Documents" folder on their computers or that they did so. (CCFF ¶¶ 1354-1358, 1361, 1363-1372, 1375-1378).

Monitor Security Software Settings and Operating System Updates Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Monitor Security Software Settings and Operating System Updates Policy was "in practice" starting in 2002 and the suggestion that it adequately protected Personal Information on LabMD's network. The policy on its face required LabMD to routinely manually check employee computers to ensure that the Trend Micro antivirus program was updated and working and the Windows firewall setup checked to verify certain functions were enabled, including the firewall and automatic updates. (CX0006 (LabMD Policy Manual) at 13).

First, LabMD used the ClamWin and AVG antivirus programs on employee computers until late 2009 (CCFF ¶ 566-567, 581, 584), not Trend Micro. (CX0608 (Emails between TrendMicro, Boyle, Daugherty, Kaloustian, et al) at 2). And to the extent that LabMD could claim that the policy applies to the ClamWin and AVG programs, LabMD nonetheless did not ensure that the programs were working correctly by regularly updating their virus definitions or conducting or reviewing antivirus scans on employee computers to check for vulnerabilities. (CCFF ¶¶ 527-529, 532-536, 566-609). Second, LabMD did not enable the software firewall included in the Windows operating system running on employee computers until 2007 at the earliest, preventing the firewalls from protecting the computers. (CCFF ¶¶ 1085, 1088-1091; *see* CX0006 (LabMD Policy Manual) at 13 (1.a.ii, 1.b)). Lastly, LabMD's manual inspections of employee computers for compliance with the policy were haphazard and ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696).

Password Policy: The proposed finding is misleading as to the claim that the Password Policy was "in practice" starting in 2002. In connection with the Employee User Account Policy (CX0006 (LabMD Policy Manual, at 12), and the Client User Account Policy (CX0006, (LabMD Policy Manual, at 9), the Password Policy facially required each employee and each "individual client employee" to have a unique password to limit their access to LabMD's network to the information needed to do their jobs. (CX0006 (LabMD Policy Manual, at 14).

The "in practice" claim is contradicted by the weight of the evidence. LabMD allowed non-unique passwords by allowing a number of employees to use "labmd" as their password or to share passwords that could be used to access Personal Information. (CCFF ¶¶ 947-951, 957-970). Similarly, it allowed individual employees of physician clients to choose their own passwords, including at times their own initials, and to share passwords, without reviewing whether the passwords were secure. (CCFF ¶¶ 974-983).

Risk Assessment and Vulnerability Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Risk Assessment and Vulnerability Policy was "in practice" starting in 2002.

The Risk Assessment and Vulnerability Policy sets out how LabMD assessed the risk of security vulnerabilities and remediated them. (CX0006 (LabMD Policy Manual) at 15). It incorporated by reference the Monitor Security Software Settings and Operating System Updates Policy for employee computers and servers. (CX0006 (LabMD Policy Manual) at 15). It also required using Trend Micro to monitor security status and settings, defenses, scans, and updates of software on employee computers and LabMD servers. (CX0006 (LabMD Policy Manual) at 15).

As to employee computers, the "in practice" claim is contradicted by the weight of the evidence because LabMD used the ClamWin and AVG antivirus programs on employee computers until late 2009 (CCFF ¶ 566-567, 581, 584), not Trend Micro. (CX0608 (Emails between TrendMicro, Boyle, Daugherty, Kaloustian, et al) at 2). Even to the extent that the "in practice" claim could apply to LabMD's use of ClamWin and AVG antivirus programs, the proposed finding is contradicted by the weight of the evidence because did not regularly update ClamWin and AVG virus definitions on employee computers, conduct or review antivirus scans on the computers, or ensure that the programs were working correctly. (CCFF ¶¶ 527-529, 531-536, 566-609).

Further, the "in practice" claim is also contradicted by the weight of the evidence as to the additional components of the policy. Contrary to the Monitor Security Software Settings and Operating System Updates Policy, LabMD did not enable the software firewall included in the Windows operating system running on employee computers until 2007 at the earliest, so that the firewall could not be used to assess risk. (CCFF ¶¶ 642, 656-657, 1085, 1088-1091). It also did not routinely update the operating system on employee computers. (CCFF ¶ 1000). LabMD's manual inspections of employee computers for compliance with this policy, including the Monitor Security Software Settings and Operating System Updates Policy, were both haphazard and ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696).

As to servers, the "in practice" claim is contradicted by the evidence until at least 2006 because LabMD used the Norton/Symantec antivirus program, not Trend Micro, on servers until then. (CCFF ¶¶ 539, 550). To the extent that the "in practice" claim applies to the Norton/Symantec antivirus program, the proposed finding is contradicted by the weight of the evidence. LabMD used the Norton/Symantec program even after Norton stopped supporting it

by providing new virus definitions, so that the program was incapable of identifying risks presented by newly discovered viruses. (CCFF ¶ 547-550). LabMD did not consistently update the program's virus definitions when they were available, use it to conduct scans of servers, or review the results to address risks that the program discovered. (CCFF ¶¶ 541-563).

Further, to the extent that the "in practice" claim applies beyond the antivirus programs on servers, the proposed finding is contradicted by the weight of the evidence. LabMD at times disabled the software firewall included in the Windows operating system running on servers, preventing them from being used to identify risks. (CCFF ¶ 642-656, 1087). Additionally, until at least 2010 LabMD did not timely update operating systems and applications to address vulnerabilities. (CCFF ¶¶ 996-999, 1003-1040).

Security Assignment and Accountability Policy: Complaint Counsel has no specific response to the proposed finding that the Security Assignment and Accountability Policy required IT employees to provide employees and physician clients with user names and passwords to access computers, email, and the laboratory and billing systems, or that they did so.

Server Monitoring Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Server Monitoring Policy was "in practice" starting in 2002. The Server Monitoring Policy required at least daily reviews of server operation, functionality, security settings, and programs (including security programs, scans, and updates), and Windows operating system updates, and resolving error and warning messages. (CX0006 (LabMD Policy Manual) at 17). First, LabMD used the Norton/Symantec antivirus program on servers until at least late 2006. (CCFF ¶¶ 539, 550). It used the Norton/Symantec program even after Norton stopped supporting it by providing new virus definitions, so that the program was not timely updated and could not identify for newly discovered viruses. (CCFF ¶ 547-550). LabMD also

did not consistently update the program's virus definitions when they were available, use it to conduct scans of servers, or review the results to address risks that the program discovered. (CCFF ¶¶ 541-549, 553-563). Second, LabMD at times disabled the Windows operating system software firewall on servers, preventing them from protecting the servers. (CCFF ¶ 642-656, 1087). Until at least 2010 LabMD did not timely update operating systems and applications to address vulnerabilities. (CCFF ¶¶ 996-999, 1003-1040).

Software Monitoring Policy: The proposed finding is contradicted by the weight of evidence as to the claim that the Software Monitoring Policy was "in practice" starting in 2002. The Software Monitoring Policy required routinely reviewing the operation of security programs on employee computers (including conducting and reviewing scans, resolving error and warning messages, and ensuring that the latest updates had been installed) as well as reviewing applications on computers to remove inappropriate applications. (CX0006 (LabMD Policy Manual) at 18). LabMD did not regularly update virus definitions on employee computers, conduct or review antivirus scans on the computers, or ensure that the antivirus programs were working correctly. (CCFF ¶¶ 527-536, 566-578, 582-609). LabMD's manual inspection of employee computers for compliance with the policy were haphazard and ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696).

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)).

Response to Finding No. 98:

To the extent that it suggests that the Client User Account Policy and Audit Security Operations and Internet Connectivity Policy were set out in writing in 2003, the proposed finding is contradicted by the weight of the evidence. CX0006, including these policies, did not exist in

writing until 2010 (CCFF ¶¶ 446-448), thus these policies were not available to guide LabMD employees until 2010. A comprehensive information security program should be in writing to provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes as threats evolve. (CCFF ¶ 411).

Client User Account Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Client User Account Policy was "in practice" starting in 2003. The Client User Account Policy facially required LabMD to assign unique user names and passwords to each user in physician-client offices to use to access LabMD's network. (CX0006 (LabMD Policy Manual, at 9). LabMD allowed individual employees of physician clients to choose their own passwords, including at times their own initials, and to share passwords, without reviewing whether the passwords were secure. (CCFF ¶¶ 974-983).

Audit Security Operations and Internet Connectivity Policy: The proposed finding is contradicted by the weight of the evidence as to the claim that the Audit Security Operations and Internet Connectivity Policy was "in practice" starting in 2003. The Audit Security Operations and Internet Connectivity Policy required IT employees to conduct and review Trend Micro scans of servers and employee computers, verify that Trend Micro was working and timely updated, and review and appropriately limit the internet connectivity of servers and employee computers. (CX0006 (LabMD Policy Manual) at 8).

As to servers, the "in practice" claim is contradicted because until at least 2006 LabMD used the Norton/Symantec antivirus program, not Trend Micro, on servers. (CCFF ¶¶ 539, 550). To the extent that the "in practice" claim could apply to the Norton/Symantec antivirus program, the proposed finding is contradicted by the weight of the evidence because LabMD used the Norton/Symantec program even after Norton stopped supporting it by providing new virus

definitions, so that the program was incapable of identifying risks presented by newly discovered viruses. (CCFF ¶ 547-550). Further, LabMD did not consistently update the program's virus definitions when they were available, use it to conduct scans of servers, or review the results to address risks that the program discovered. (CCFF ¶¶ 541-549, 553-563).

To the extent the "in practice" claim applies to employee computers, the proposed finding is contradicted because LabMD used the ClamWin and AVG antivirus programs on employee computers until late 2009 (CCFF ¶¶ 566-567, 581, 582, 584), not Trend Micro. (CX0608 (Emails between TrendMicro, Boyle, Daugherty, Kaloustian, et al) at 2). However, to the extent that the "in practice" claim of the proposed finding could apply to the ClamWin and AVG antivirus programs LabMD actually used, the proposed finding is contradicted by the weight of the evidence. LabMD did not ensure that the programs were working correctly on employee computers by regularly updating their virus definitions and conducting and reviewing antivirus scans on the computers. (CCFF ¶¶ 527-529, 531-536, 567-609).

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)).

Response to Finding No. 99:

The proposed finding is not supported by the citation to the record. LabMD's Policy Manual includes a "Use Policy," but not an "Acceptable Use and Security Policy." (CX0006 (LabMD Policy Manual) at 3-7). To the extent the proposed finding applies to the Use Policy, and implies that this policy was set out in writing in 2004, it is contradicted by the weight of the evidence. CX0006, including the "Use Policy," did not exist in writing until 2010 (CCFF ¶¶ 415-417, 446-448), thus neither the manual nor the policy was available to guide LabMD employees until 2010. A comprehensive information security program should be in writing to

provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes as threats evolve. (CCFF ¶ 411).

To the extent the proposed finding asserts the Use Policy was "in practice" effective 2004, the proposed finding is contradicted by the weight of the evidence. The policy prohibits unauthorized disclosure of information, downloading and installing unauthorized files and programs (including file sharing programs), using LabMD equipment except for work purposes, and sharing passwords and not periodically changing them (CX0006 (LabMD Policy Manual) at 3-5), and recommends that employees encrypt emails with sensitive information. (CX0006 (LabMD Policy Manual) at 6). It also states that LabMD will enforce the policy and its prohibitions by using tools to log network traffic, monitor its content, block viruses, and ensure security and compliance with the policy. (CX0006 (LabMD Policy Manual) at 3, 7). The weight of evidence contradicts the proposed finding that this policy was "in practice" starting in 2004 as follows:

Logging Traffic and Monitoring Content: Notwithstanding the "Monitoring of Internet Use" Section of the Use Policy (CX0006 (LabMD Policy Manual) at 3), LabMD's network firewall had very little capacity for logging network traffic, LabMD did not log activity on employee computers or use tools capable of inspecting the content of network traffic, and, in any event, LabMD did not review the inadequate logs it had. (CCFF ¶¶ 637-639, 642-648, 651-657, 699-702). LabMD did not properly configure its network firewall to block unwanted traffic and, at times, disabled the software firewall included in the Windows operating system running on servers, preventing them from being used to control inappropriate Internet connections and downloads to and from servers. (CCFF ¶¶ 631-635, 1075-1082, 1085-1087, 1094-1105). In addition, LabMD did not properly configure software firewalls on employee computers to block

unwanted traffic and, at times, disabled them, preventing them from being used to control inappropriate Internet connections and downloads to and from employee computers. (CCFF ¶¶ 1075-1082, 1085, 1088-1091).

Passwords: Notwithstanding the language of the "Account and Password Security" section of the Use Policy (CX0006 (LabMD Policy Manual) at 5), LabMD did not prevent employees from sharing passwords or require them to change passwords. (CCFF ¶¶ 947-951, 957-970).

Email Encryption: Notwithstanding the "Email Security and Encryption" Section of the Use Policy (CX0006 (LabMD Policy Manual) at 6), LabMD had no policy requiring encrypting sensitive information in emails between 2004 and at least August 2009. (CCFF ¶¶ 474-477). Nor did it provide tools employees could use to encrypt emails or train them to do so. (CCFF ¶¶ 478-479). Furthermore, between 2004 and at least October 2006, sensitive information, including billing information and insurance codes, was sent unencrypted from LabMD's network to Mr. Daugherty's personal AOL email account. (CCFF ¶ 480).

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)).

Response to Finding No. 100:

To the extent the proposed finding sets forth a quotation from LabMD's Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it is not supported by the citation to the record. The Employee Handbook does not state, or in any other way prove, that LabMD informed employees of new policies, if any new policies were implemented. The Handbook only informs employees that

they "will be expected to cooperate" with any such new policies, assuming they were informed of them. (CX0001 (LabMD Employee Handbook Rev. June 2004) 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)).

Response to Finding No. 101:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. Otherwise, the proposed finding is contradicted by the weight of the evidence. LabMD did not provide adequate security training to IT and non-IT employees. (CCFF ¶¶ 441-443, 852-900). The only training LabMD did provide to some employees, Compliance Training—like the Handbook—merely alluded to other instruction LabMD would provide on security and privacy policies and procedures. (CCFF ¶¶ 872-876). That instruction never occurred. (CCFF ¶¶ 441-443, 879-884).

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)).

Response to Finding No. 102:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it calls for a legal conclusion. Finding whether the quoted text constitutes the Mission Statement of the corporation LabMD, Inc.—as opposed to some text LabMD decided to insert at the beginning of its manual—would require considering corporate requirements and facts outside the record that are irrelevant to this proceeding. Furthermore, to the extent the proposed finding asserts that LabMD was "fully compliant with the rules, laws and guidelines regulating its business," that conclusion is not supported by the citation to the record,

and is contradicted by the preponderance of the evidence that LabMD violated Section 5 of the FTC Act. To the extent the proposed finding asserts LabMD's intent as a corporation to comply with the law, it is irrelevant because intent is not an element of a Section 5 violation. (CCCL ¶ 12).

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)).

Response to Finding No. 103:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it calls for a legal conclusion, and is not supported by the record. Finding whether the quoted text constitutes the Purpose of the corporation LabMD, Inc.—as opposed to some text LabMD decided to insert at the beginning of its manual—would require considering corporate requirements and facts outside the record that are irrelevant to this proceeding. To the extent the proposed finding asserts LabMD's intent as a corporation, it is irrelevant because intent is not an element of a Section 5 violation. (CCCL ¶ 12). Furthermore, to the extent the proposed finding asserts that LabMD took any of the steps listed in the quoted text, the Court should disregard the proposed finding because it is not supported by the citation to the record, and is contradicted by the weight of the evidence. The evidence proves that

LabMD failed to "provide mechanisms and resources broad enough to accomplish this objective," because it failed to provide reasonable security for Personal Information on its computer network (CCFF ¶¶ 382-1110 (§ 4 LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Network)), despite the availability of free and low-cost measures (CCFF ¶¶ 1113-1185 (§ 5 LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures)). Likewise, with regard to protecting Personal Information it collected and maintains, LabMD failed to "keep[] employees and business associates educated, informed and trained." (CX0001 (LabMD Employee Handbook Rev. June 2004) at 3; *see* CCFF ¶¶ 852-900).

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)).

Response to Finding No. 104:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and calls for a legal conclusion. To the extent the proposed finding asserts that the Employee Handbook placed a legal or contractual obligation on employees, it calls for a legal conclusion, and is not supported by the citation. The proposed finding is also not supported because the proposition it offers is not stated anywhere in the Employee Handbook and cannot be reasonably inferred from the Handbook as a whole. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 1-23).

Furthermore, the proposed finding is misleading and contradicted by the weight of the evidence to the extent it asserts that, because LabMD's handbook included the Statement of Purpose and Ethics, LabMD took reasonable steps to ensure that its employees complied with the law. The Statement itself purports to set out a plan for implementation, which include: "keeping

employees . . . educated, informed, and trained," making "compliance everyone's job," and LabMD establishing "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 and LabMD policies" and providing "mechanisms and resources broad enough to accomplish this objective." (CX0001 (LabMD Employee Handbook Rev. June 2004) at 3). But LabMD systematically failed to meet its own standard. For instance, the handbook claims that LabMD took "specific measures to ensure our compliance" with HIPAA. CX0001 (LabMD Employee Handbook rev. June 2004) at 6. However, no LabMD employee, including Mr. Daugherty, was able to identify a single security measure taken to ensure HIPAA compliance. (CCFF ¶¶ 427-431).

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)).

Response to Finding No. 105:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and calls for a legal conclusion. To the extent the proposed finding asserts that the Employee Handbook placed a legal or contractual obligation on employees, it calls for a legal conclusion, and is not supported by the citation. The proposed finding is also not supported because the proposition it offers is not stated anywhere in the Employee Handbook and cannot be reasonably inferred from the Handbook as a whole. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 1-23). Likewise, no "Standards of Conduct" appear in the cited document. Furthermore, the proposed finding is misleading and contradicted by the weight of the evidence to the extent it asserts that, because LabMD's handbook included the Statement of Purpose and

Ethics, LabMD took reasonable steps to ensure that its employees complied with the law. (CCRRFF ¶104).

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)).

Response to Finding No. 106:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 107:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. However, to the extent the proposed finding asserts that LabMD took "specific measures to ensure [LabMD's] compliance with [HIPAA]" (CX0001 (LabMD Employee Handbook Rev. June 2004) at 6), the Court should disregard it because it is not supported by the citation to the record, and is contradicted by the weight of evidence. No LabMD employee, including Mr. Daugherty, was able to identify a single measure taken to ensure HIPAA compliance. (CCFF ¶¶ 427-431, 897-898). Furthermore, the statement is titled "Privacy of Protected Information," and no evidence in the record supports that it was intended

to relate to security. Regardless, the proposed finding is irrelevant because HIPAA is irrelevant to this case. (*See* CCRRFF ¶¶ 298-99).

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)).

Response to Finding No. 108:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 109:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 110:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. To the extent the proposed finding asserts that LabMD did "safeguard [employee health and medical records] from disclosure" and "divulge[d] such information only as allowed or required by law and in accordance with HIPAA Privacy guidelines," the Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 111:

All Policies and Plan: To the extent the proposed finding asserts that the stated policies were set out in writing in 2008, it is contradicted by the weight of evidence. The PC System Setup To Prevent Downloading Files From Internet Policy, Prohibit Use Of File–Sharing Software Policy, and Security Incident Response Plan (CX0006 (LabMD Policy Manual) at 20-22), did not exist in writing until 2010 (CCFF ¶¶ 415-417, 446-448), therefore neither the manual nor the policies and plan were available to guide LabMD employees until 2010. A comprehensive information security program should be in writing to provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes as threats evolve. (CCFF ¶ 411).

PC System Setup To Prevent Downloading Files From Internet Policy: The proposed finding is contradicted by the weight of evidence as to the claim that the PC System Setup To Prevent Downloading Files From Internet Policy ("Download Policy") was "in practice" starting in 2008. The Download Policy required IT employees to set up on each employee computer an administrative user profile and an employee user profile. (CX0006 (LabMD Policy Manual) at 20; *see also* CX0006 (LabMD Policy Manual) at 12 (Employee User Account Policy, describing employee user setup process)). The administrative user profile was to include administrative rights to the computer, including the ability to download and install programs, and was to be used only by administrators. (CX0006 (LabMD Policy Manual) at 20). The employee user profile was to include employee rights, which do not include the ability to download and install programs, and was to be used by non-administrative employees. (CX0006 (LabMD Policy Manual) at 20). But until at least November 2010, LabMD gave many

employees administrative rights over their computers, so that they had the ability to change security settings on the computers and download programs and files to the computers. (CCFF ¶¶ 458-462, 880-881, 1050-1063).

Prohibit Use Of File–Sharing Software Policy: The proposed finding is contradicted by the weight of evidence as to the claim that the Prohibit Use Of File–Sharing Software Policy ("File-sharing Policy") was "in practice" starting in 2008. Like the Download Policy, the File-Sharing Policy required IT employees to set up on each employee computer an administrative user profile and an employee user profile. (CX0006 (LabMD Policy Manual) at 21). But until at least November 2010, LabMD gave many employees administrative rights over their computers, so that they had the ability to change security settings on the computers and download programs and files to the computers. (CCFF ¶¶ 458-462, 880-881, 1050-1063).

Security Incident Response Plan: The proposed finding is contradicted by the weight of evidence as to the claim that the Security Incident Response Plan was "in practice" starting in 2008. To the extent the Security Incident Response Plan requires LabMD to implement "[a]ppropriate systems for watching, identifying, and alerting" (CX0006 (LabMD Policy Manual) at 22), it is contradicted by the weight of the evidence. First, it did not use an Intrusion Detection System, an Intrusion Protection System, or file integrity monitoring products at all (CCFF ¶¶ 514-521, 699-702, 705-712), and only began conducting penetration tests in 2010, with telling results. (CCFF ¶¶ 715-808, 996-1004, 1011-1040). Second, the measures it relied on to detect risks—antivirus programs, firewalls, and manual inspections—were also ineffective. (CCFF ¶¶ 524-696 (§ 4.3.2 LabMD Could Not Effectively Assess Risks Using Only Antivirus Applications, Firewalls, and Manual Inspections)).

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)).

Response to Finding No. 112:

To the extent the proposed finding sets forth a quotation from LabMD's Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it is not supported by the citation to the record. (CCRRFF ¶ 100 (addressing substantively identical Proposed Finding 100 regarding CX0001 (LabMD Employee Handbook Rev. June 2004))).

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)).

Response to Finding No. 113:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it calls for a legal conclusion. (CCRRFF ¶ 102 (addressing substantively identical Proposed Finding 102 regarding CX0001 (LabMD Employee Handbook rev. 2004))).

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)).

Response to Finding No. 114:

To the extent the proposed finding references content from the Employee Handbook, Complaint Counsel has no specific response. Otherwise, the Court should disregard the proposed finding because it calls for a legal conclusion, and is not supported by the record. (CCRRFF ¶ 103 (addressing substantively identical Proposed Finding 103 "Purpose" with regard to CX0001 (LabMD Employee Handbook rev. 2004))).

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)).

Response to Finding No. 115:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and calls for a legal conclusion. (CCRRFF ¶ 104 (addressing substantively identical Proposed Finding 104 regarding CX0001 (LabMD Employee Handbook rev. 2004))).

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)).

Response to Finding No. 116:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and calls for a legal conclusion. (CCRRFF ¶ 105 (addressing substantively identical Proposed Finding 105 regarding CX0001 (LabMD Employee Handbook rev. 2004)).

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)).

Response to Finding No. 117:

To the extent the proposed finding is a quotation from the Employee Handbook, Complaint Counsel has no specific response. However, to the extent the proposed finding asserts that LabMD took "specific measures to ensure [LabMD's] compliance with [HIPAA] (CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 6), the Court should disregard it because it is not supported by the citation to the record, and is contradicted by the weight of evidence. No

LabMD employee, including Mr. Daugherty, was able to identify a single measure taken to ensure HIPAA compliance. (CCFF ¶¶ 427-431, 897-898). Furthermore, the statement is titled "Privacy of Protected Information," and no evidence in the record supports that it was intended to relate to security. Regardless, the proposed finding is irrelevant because HIPAA is irrelevant to this case. (*See* CCRRFF ¶¶ 298-99).

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 on-site computers 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)).

Response to Finding No. 118:

Complaint Counsel has no specific response

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)).

Response to Finding No. 119:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 120:

The Court should disregard the proposed finding because it not supported by the citation to the record. The cited document does not state any date on which the contained policies were "effective." Moreover, as of June 4, 2010, three training policies contained in the Manual

(CX0007/RX074[9]) were still "to be done." (CX0444 (LabMD Access Letter Response by Philippa Ellis) at 1-2). The policies yet to be done were Education and Training – Anti–Virus and Anti–Spyware Applications, Education and Training – Instruction for Closing Network Connections, and Education and Training – Instruction of P2P Applications. (CX0444 (LabMD Access Letter Response by Philippa Ellis) at 1-2).

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)).

Response to Finding No. 121:

The proposed finding is contradicted by the weight of the evidence for the following reasons. First, prior to mid-2010, none of the policies were written. (CCFF ¶¶ 415-417, 446-448). A comprehensive information security program should be in writing to provide guidance to those implementing it, to provide instruction to employees, and to record current security goals and practices to facilitate changes as threats evolve. (CCFF ¶ 411). Second, to the extent the proposed finding asserts that the policies were "utilized" for the period from 2001 to 2010,

[9] Although RX074 appears at a different Bates range than CX0007, and was therefore not addressed in the parties' Duplicate CX and RX Exhibit Index, both are LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual. They are identical but for the Bates stamps.

the evidence demonstrates that they were not. (CCRRFF ¶ 96 ("(11) Employee User Account Policy" not in practice), ¶ 97 ("(6) Desktop Monitoring Policy," "(12) Monitor Security Software Settings and Operating System Updates Policy," "(13) Password Policy," "(16) Risk Assessment and Vulnerability Policy," "(19) Server Monitoring Policy," and "(20) Software Monitoring Policy" not in practice), ¶ 98 ("(3) Audit Security Operations and Internet Connectivity Policy" and "(4) Client User Account Policy" not in practice), ¶ 99 ("(1) Acceptable Use and Security Policy" not in practice), ¶ 111 ("(14) PC System Setup To Prevent Downloading Files From Internet Policy," "(15) Prohibit Use of File–Sharing Software Policy," and "(18) Security Incident Response Plan" not in practice)). Third, the proposed finding is not supported by the citation to the record for several of the policies the proposed finding asserts were "utilized in practice." On the contrary, the cited exhibit states that "(2) Assessment – Audit Policy" was not "in practice" until the second quarter of 2010. (CX0445 (LabMD Access Letter Response by Philippa Ellis) at 4). Similarly, the cited document states that the following policies were still "[t]o be done" at the date of the letter (July 16, 2010), and predicts they will be adopted in the third quarter of 2010: "(8) Education and Training – Anti–Virus and Anti–Spyware Applications," "(9) Education and Training – Instruction for Closing Network Connections," and "(10) Education and Training – Instruction of P2P Applications." (CX0445 (LabMD Access Letter Response by Philippa Ellis) at 5).

To the extent the proposed finding asserts that the "(5) Data Backup Policy," "(7) Document Backup Software Policy," and "(17) Security Assignment and Accountability Policy" were in practice, Complaint Counsel has no specific response.

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

Response to Finding No. 122:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Dr. Hill's cited testimony was limited to stating that she considered the 2004 LabMD Employee Handbook's prohibition of using LabMD computers for personal internet or email, (CX0001 (LabMD Employee Handbook Rev. June 2004) at 7) a policy, not unspecified information in the handbook as a whole. While Dr. Hill considered the prohibition to be a policy (Hill, Tr. 289), Dr. Hill also noted that it was inadequate because it did not communicate a security goal or the security consequences of violating the policy. (Hill, Tr. 289-292).

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)).

Response to Finding No. 123:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 124:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 125:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 126:

The proposed finding is misleading, because Mr. Dooley testified that LabMD had a firewall installed, but was not qualified to opine on data security and did not describe how the firewall protected against intrusions. (CX0711 (Dooley, Dep. at 24, 31)). Mr. Dooley testified that LabMD used a variety of antivirus software, including some that were not centrally managed. (CX0711 (Dooley, Dep. at 72)). Antivirus programs that are not centrally managed prevent IT employees from remotely updating the software with current virus definitions, scanning computers, and viewing and remedying issues that are discovered. (CCFF ¶ 569). Instead, they rely on employees to take these steps and report warnings. (CCFF ¶ 570). In addition, the cited testimony does not support the dates of Mr. Dooley's employment.

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)).

Response to Finding No. 127:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 128:

Complaint Counsel has no specific response.

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

Response to Finding No. 129:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 130:

Complaint Counsel has no specific response.

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

Response to Finding No. 131:

Mr. Dooley's testimony refers to "LabSoftware." (CX0711 (Dooley, Dep. at 125)). However, Complaint Counsel acknowledges that LabMD used LabSoft. (CCFF ¶¶ 226-232).

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)).

Response to Finding No. 132:

The proposed finding is misleading to the extent it suggests Mr. Dooley testified that LabMD had firewalls that protected against intrusion. (CCRRFF ¶ 126).

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

Response to Finding No. 133:

The Court should disregard the proposed finding because it is contradicted by the weight of the evidence. The evidence shows that LabMD's router was not configured to provide firewall protection at its Powers Ferry Road location. (CCFF ¶ 1086). Mr. Dooley's perception otherwise should not be weighted because he does not have expertise in that area. Mr. Dooley, who is not a security expert, testified that a firewall router is "a device that has – as incoming Internet traffic is received, it routes that." (CX0711 (Dooley, Dep. at 24, 31)). His description only covers routing functions—Mr. Dooley does not describe any firewall functions, such as blocking unwanted traffic or blocking traffic to unauthorized applications. (CX0711 (Dooley, Dep. at 24); *see also, e.g.*, CCFF ¶¶ 1075-1081 (describing the functions of firewalls)).

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

Response to Finding No. 134:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Dooley testified that "we had outside contractors that were *supposedly* tasked with those responsibilities." (CX0711 (Dooley, Dep. at 39) (emphasis added)). Mr. Dooley testified that he did not know what the outside contractors' responsibilities, including APT, were. (CX0711 (Dooley, Dep. at 39)). He also testified that he did not interact with them much and did not know how the outside contractors assessed risks at LabMD. (CX0711 (Dooley, Dep. at 39-40)).

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)).

Response to Finding No. 135:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 136:

To the extent the proposed finding asserts when APT began providing services, Complaint Counsel has no specific response. To the extent it asserts that APT provided services in 2008 or 2009, it is contradicted by the weight of the evidence. Mr. Truett provided contradictory testimony regarding the time period in which he provided services to LabMD. He testified that he provided services to LabMD through March 2007, and could not recall if APT provided services after that date. (CX0731 (Truett, Dep. at 49-50)). Later, he stated that APT stopped providing services to LabMD "around 2008 or 2009 or whenever – somewhere around the date that was in the affidavit." (CX0731 (Truett, Dep. at 72-73)).

Mr. Truett's earlier testimony that APT ceased to provide service to LabMD in March 2007 comports to the additional record evidence. In late 2006 and 2007, LabMD replaced APT's services with additional internal IT employees that it hired. (CX0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions) at 1; CX0733 (Boyle, IHT at 64-65); CX0731 (Truett, Dep. at 28-29)). Furthermore, Christopher Maire testified that LabMD did not use outside contractors during his tenure as an IT employee for LabMD, which began in mid-2007. (CX0724 (Maire, Dep. at 105); CCFF ¶¶ 357-358).

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)).

Response to Finding No. 137:

The proposed finding is misleading to the extent it suggests LabMD adopted and fully implemented APT's recommendations. Mr. Truett testified only that APT made recommendations to LabMD. (CX0731 (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)).

Response to Finding No. 138:

The proposed finding is misleading to the extent it suggests APT reviewed LabMD's network traffic on an ongoing basis for data security purposes. Mr. Truett testified that "[w]e didn't do any monitoring or log reviews unless it was ad hoc," that any such ad hoc reviews conducted were to resolve a non-security issue such as "Internet speeds, connectivity problems," and that APT did not provide log review as a service. (CX0731 (Truett, Dep. at 69)). Mr. Dooley testified that he was not familiar with any network diagnostic tools, and knew only that APT was looking at "different traffic and things." (CX0711 (Dooley, Dep. at 52)).

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

Response to Finding No. 139:

The Court should disregard the proposed finding, to the extent it suggests the citation supports a claim that APT installed and managed antivirus software *for LabMD*, because it is not supported by the citations to the record.

Mr. Truett testified that installing and implementing network firewall equipment in front of Internet connections and installing antivirus software were the types of services APT provided to the businesses for whom it provided consulting services. (CX0731 (Truett, Dep. at 18-19)). The citation does not state that Mr. Truett provided these services to LabMD.

Mr. Dooley stated that APT installed "managed antivirus software," but did not testify that APT managed that antivirus software. (CX0711 (Dooley, Dep. at 71-72)). He also testified that the antivirus software at off-site computers at client locations could not be centrally managed. (CX0711 (Dooley, Dep. at 72).

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

Response to Finding No. 140:

To the extent the proposed finding asserts that APT provided backup software, the Court should disregard it because it is not supported by the citation. The proposed finding is also misleading to the extent it suggests APT applied patches at LabMD. APT merely verified that patches were installed when on-site in response to a breakdown or problem, but did not affirmatively patch servers or workstations.

Mr. Truett could not recall how service packs and software patches were applied at LabMD. (CX0731 (Truett, Dep. at 32)). He stated that APT's general practice would be to go to

a client site to handle a breakdown or fix issues that had come up, and at that time to "verify[]that patches and updates were loaded specifically servers but also try to check workstations." (CX0731 (Truett, Dep. at 32)). This involved physically examining the server console to "verify" that patches were installed. (CX0731 (Truett, Dep. at 32)).

Mr. Dooley testified that he was not involved in patching. (CX0711 (Dooley, Dep. at 114)). He testified that LabMD employee Pat Howard (CCFF ¶¶ 333-338), or APT would be responsible for patching. (CX0711 (Dooley, Dep. at 114)). He did not testify that APT actually applied any patches to software. (CX0711 (Dooley, Dep. at 114)).

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

Response to Finding No. 141:

To the extent the proposed finding asserts that APT specialized in the medical field for the entire time it served LabMD, the proposed finding is contradicted by the evidentiary record. Mr. Truett testified that the majority of his clients were not in the medical industry. (CX0731 (Truett, Dep. at 37-38)).

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)).

Response to Finding No. 142:

The proposed finding is contradicted by the weight of the evidence. Mr. Truett did not recall doing an evaluation of LabMD's antivirus system. (CX0731 (Truett, Dep. at 33)). In fact, Mr. Truett did not recall ever providing any specific evaluation regarding the criticality of potential risks to his clients' networks, and did not recall doing any assessment of potential risks and vulnerabilities associated with LabMD's network. (CX0731 (Truett, Dep. at 118-119)). APT installed a firewall on LabMD's system, but did not testify to doing an evaluation of LabMD's firewall system. (CX0731 (Truett, Dep. at 33)).

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)).

Response to Finding No. 143:

The Court should disregard the proposed finding because it is not supported by the citation to the record. There is no location identified as "Ex. 5" within CX0447. To the extent the proposed finding cites to the text of CX0447, it is contradicted by other evidence in the record. Mr. Truett testified that APT identified a problem with LabMD's server, without specifying which server, on May 3, 2006. (CX0731 (Truett, Dep. at 142)). Mr. Truett stated that the APT engineer found that the antivirus program on the server would not run virus scans, and had not updated its virus definitions for almost a year, since July 2005. (CX0731 (Truett, Dep. at 142)). Mr. Truett did not testify that the problem was resolved or remedied. (CX0731 (Truett, Dep. at 142)).

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

Response to Finding No. 144:

The proposed finding is contradicted by the weight of the evidence. APT identified, but did not solve, a problem with antivirus protection on a LabMD server in May 2006. (CCRRFF ¶ 143). On June 21, 2006, APT identified that the antivirus program on LabMD's servers had not updated for over a month, and would not manually update. (CX0035 (APT Service Invoice) at 3). APT did not resolve this problem, either. (CX0035 (APT Service Invoice) at 3). APT made recommendations on upgrading antivirus software (CX0731 (Truett, Dep. at 42-43)), but did not manage LabMD's antivirus software. (CCRRFF ¶ 139).

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)).

Response to Finding No. 145:

The Court should disregard the proposed finding because it is not supported by the citation to the record. There is no location identified as "Ex. 5" within CX0447.

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)).

Response to Finding No. 146:

The Court should disregard the proposed finding because it is not supported by the citation to the record. There is no location identified as "Ex. 4" within CX0447.

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)).

Response to Finding No. 147:

The proposed finding is misleading to the extent it suggests the ZyWALL firewall provided special protection to medical data. Mr. Truett did not testify that the ZyWALL firewall was specific to APT's medical clients; rather, he testified that the ZyWALL equipment was what "we sold to most of our medical clients." (CX0731 (Truett, Dep. at 31)).

The cited evidence does not support the proposition that APT provided another firewall application for LabMD during the 2006-2008 time period. Mr. Truett testified that he "believe[d]" APT sold LabMD two firewalls, did not know if they were sold at the same time or not, and did not specify the date. (CX0731 (Truett, Dep. at 31); *see also* CCRRFF ¶ 136 (APT ceased providing services to LabMD around March 2007)).

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)).

Response to Finding No. 148:

The proposed finding is misleading to the extent it suggests APT provided data security services in connection with the administration of servers and firewalls. Mr. Truett testified that APT's work concerning the administration of servers and firewall systems would be limited to "maybe a user management function, a user forgot their password." (CX0731 (Truett, Dep. at 31-32)).

The proposed finding is misleading to the extent it suggest APT applied patches at LabMD. APT merely verified that patches were installed when on-site in response to a breakdown or problem, but did not affirmatively patch servers or workstations. (CCRRFF ¶ 140; CX0731 (Truett, Dep. at 32-33)).

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

Response to Finding No. 149:

Complaint Counsel has no specific response.

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

Response to Finding No. 150:

The proposed finding is contradicted by the weight of the evidence as to the time period for LabMD's installation and utilization of TrendMicro. The evidence shows that LabMD used, from at least October 2006, free antivirus program ClamWin (CCFF ¶ 567; CX0724 (Maire, Dep. at 10, 95) (testifying ClamWin used through 2008)), and a free version of AVG on employee computers (CCFF ¶¶ 581-584, 615 (LabMD used AVG during tenures of Ms. Simmons (October 2006 through August 2009), Mr. Bureau (December 2008 through April 2010), and Mr. Bradley (May 2010 through February 2014)).

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

Response to Finding No. 151:

Complaint Counsel has no specific response.

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

Response to Finding No. 152:

Complaint Counsel has no specific response.

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

Response to Finding No. 153:

The proposed finding is not supported by the citation to the record and is contradicted by the weight of the evidence. Mr. Maire testified only that LabMD had in place a "Firewall to prevent unrestricted -- restricted access to websites." (CX0724 (Maire, Dep. at 97)). In fact, the evidence shows that the software Windows firewall included in the operating system LabMD used was not deployed through 2007. (CCFF ¶¶ 1085-1091). Furthermore, LabMD did not properly configure the firewall applications it used. (CCFF ¶¶ 1094-1105).

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

Response to Finding No. 154:

The Court should disregard the proposed finding as impermissible expert testimony. Besides not being offered or qualified as an expert in this matter, Mr. Maire is not qualified to provide a lay opinion about LabMD's security. Mr. Maire did not have data security responsibilities at LabMD, but instead worked with users to "verify efficiency of their systems and troubleshoot any errors that may occur," prepare computers that were supplied to physician-

clients, and repairing and maintaining peripherals. (CX0724 (Maire, Dep. at 13-14)). Mr. Maire did not have responsibilities for LabMD's servers, and helped with firewalls only upon request. (CX0724 (Maire, Dep. at 14)).

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

Response to Finding No. 155:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Maire did not testify that LabMD had an intrusion-prevention system. He testified that LabMD "had a firewall in place to prevent unauthorized intruders into the system. (CX0724 (Maire, Dep. at 91)). On the contrary, LabMD did not implement an intrusion protection system or an intrusion detection system. (CCFF ¶¶ 699-702). The proposed finding is misleading to the extent it equates a firewall with an "intrusion prevention system," or implies that LabMD's firewall operated as such. Mr. Maire is not an expert in data security. (CCRRFF ¶¶ 154, 254.) Furthermore, to the extent LabMD's firewalls were providing protection again intrusion, the evidence shows that LabMD's firewall applications were deployed haphazardly or not at all and were not properly configured. (CCFF ¶¶ 631-657, 1075-1105).

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)).

Response to Finding No. 156:

The Court should disregard the proposed finding because it is not supported by the citation to the record, except to the extent that it states that LabMD used TrendMicro anti-virus software at some points during the Relevant Time Period and on some computers.

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)).

Response to Finding No. 157:

The proposed finding is misleading to the extent that it suggests that APT performed services for LabMD throughout the Relevant Time Period because it is contradicted by the weight of the evidence. In 2006 or 2007, LabMD replaced APT with LabMD employees. (CCFF ¶ 190). Furthermore, APT did not manage or secure LabMD's internal network or assess risks and vulnerabilities. (CCFF ¶¶ 182-190). APT's role was to install computers, connect them to networks, and respond to problems raised by LabMD employees, such as internet connectivity and speed. (CCFF ¶¶ 182-190).

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)).

Response to Finding No. 158:

Complaint Counsel has no specific response.

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

Response to Finding No. 159:

The proposed finding is misleading to the extent it suggests that employees were sufficiently prevented from accessing information not needed to do their jobs. Mr. Dooley testified only that LabMD's previous lab software, Intel Lab, had the capability to restrict access to certain types of information to certain users. (CX0711 (Dooley, Dep. at 127)). Mr. Dooley testified that "a cytologist in the lab wouldn't have access to the billing software." (CX0711 (Dooley, Dep. at 126)). But the fact that LabMD implemented one type of limitation does not

demonstrate that LabMD employees did not have access to quantities and types of information not needed to do their jobs. (*See* CCFF ¶¶ 811-827).

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)).

Response to Finding No. 160:

The proposed finding is contradicted by the weight of the evidence. Until November 2010, most employees had administrative access to their computers and were able to install programs on them. (CCFF ¶¶ 1050-1063). The evidence shows that after Mr. Dooley's tenure ended in 2006 (CCFF ¶ 311), most employees had administrative access to their computers. In 2007, Mr. Maire used the operating system to assign non-administrative rights to one billing department employee as a test. (CX00175 (Email Subject: Daily IT rounds, 10/22/2007); CX0176 (Email Subject: Daily IT rounds, 12/19/2007)). Several months later, Mr. Maire learned from the billing department employee to whom he had assigned non-administrative rights of a problem the employee had encountered in using the billing application. He could not resolve the problem and abandoned the effort to assign non-administrative rights to employees. (CX0176 (Email Subject: Daily IT rounds, 12/19/2007); CX0724 (Maire, Dep. at 61-63, 80-81)).

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

Response to Finding No. 161:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. Mr. Dooley testified that he is not a security expert. (CX0711 (Dooley, Dep. at 31)).

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)).

Response to Finding No. 162:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. Furthermore, APT, Mr. Truett's company, did not manage LabMD's network or provide comprehensive security services to LabMD. (CCRRFF ¶ 134, 137-140, 142-144, 146-148, 211-212; CCFF ¶¶ 182-190).

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

Response to Finding No. 163:

The proposed finding is contradicted by the weight of the evidence. LabMD managed its own data security. APT did not manage LabMD's network or provide comprehensive security services to LabMD. (CCRRFF ¶¶ 134, 137-140, 142-144, 146-148, 211-212; CCFF ¶¶ 182-190). Nor did LabMD's Internet service provider, Cypress Communications. (CCFF ¶¶ 175-180). Mr. Dooley did not identify any outside contractors that proactively identified security issues for LabMD in the cited testimony. (CX0711 (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)).

Response to Finding No. 164:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 165:

The proposed finding is misleading to the extent it suggests Ms. Harris testified her Internet access was blocked through technical means. Ms. Harris testified that she believed that her Internet access was limited to insurance companies' websites, but she did not attempt to

access any sites other than insurance companies' websites. (CX0716 (Harris, Dep. at 82-83)). She did not know if technical restrictions would have prevented her from doing so. (CX0716 (Harris, Dep. at 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)).

Response to Finding No. 166:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Ms. Harris did not testify to receiving yearly training or provide any indication of how often trainings occurred, or whether she received training more than once. (CX0716 (Harris, Dep. at 62)). Likewise, Ms. Harris testified that she did not receive any training on HIPAA (privacy and security) or the other items in LabMD's compliance program: the False Claims Act, Anti-Kickbacks, and Stark II. (CX0716 (Harris, Dep. at 62-63)). Harris testified that she received training only on limited Internet access, playing CDs, and downloading items from the Internet. (CX0716 (Harris, Dep. at 62-63)).

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)).

Response to Finding No. 167:

To the extent the proposed finding asserts that the billing system required an *additional* entry of a username and password (in addition to the log in required to the computer), Complaint Counsel has no specific response. To the extent the proposed finding asserts that the username and password employees used to log in to Lytec was or had to be different from their credential to log into their computers, the Court should disregard the proposed finding because it is not supported by the citation to the record. Ms. Harris testified that she could not remember if her

passwords were different. (CX0716 (Harris, Dep. at 68)). She testified that she tried to keep them "similar," but she thought there was "some differences." (CX0716 (Harris, Dep. at 68)).

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

Response to Finding No. 168:

Ms. Harris testified only to the extent of her knowledge on access to the Lytec billing system by non-billing personnel. (CX0716 (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)).

Response to Finding No. 169:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 170:

The proposed finding is misleading to the extent it asserts that Ms. Harris testified that all members of the billing department shredded insurance aging reports after they were done with them. Ms. Harris testified that while it was her practice to shred insurance aging reports, and that she thought others shredded them, she could not "account for what everyone else" in the billing department did with paper copies of insurance aging reports. (CX0716 (Harris, Dep. at 40-41)).

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)).

Response to Finding No. 171:

Ms. Harris testified that she was told by Jennifer Parr that Ms. Parr could see when intruders were trying to enter LabMD's servers. (CX0716 (Harris, Dep. at 130-31)). She stated

that she had no knowledge that any attempted intrusions were successful. (CX0716 (Harris, Dep. at 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)).

Response to Finding No. 172:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 173:

The Court should disregard the proposed finding because it is contradicted by the citation to the record. [Former LabMD Employee] testified that she did not shred insurance aging reports or patient aging reports, but placed them into the recycle bin. (CX0714-A ([Fmr. LabMD. Empl.], Dep. at 54-55). She did not use any shredders, nor know who used any shredders. (CX0714-A ([Fmr. LabMD. Empl.], Dep. at 54).

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)).

Response to Finding No. 174:

[Former LabMD Employee] testified that upon joining LabMD she watched a video relating to HIPAA. (CX0714-A ([Fmr. LabMD Empl.], Dep.at 86)). She did not testify to any further HIPAA training. (CX0714-A ([Fmr. LabMD Empl.], Dep.at 88))

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)).

Response to Finding No. 175:

The proposed finding is misleading and contradicted by the weight of the evidence to the extent it asserts that LabMD required employees, by policy or technical controls, to have different credentials for their computers, Lytec, and LabSoft. [Former LabMD Employee] testified that she had a different set of credentials for each system, but did not testify to LabMD's or other employees' practices. (CX 0714-A ([Former LabMD Employee], Dep. at 44-45)). Furthermore, the evidence shows that LabMD did not have policies or procedures in place to ensure employees used unique passwords. (CCFF ¶¶ 919-951).

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)).

Response to Finding No. 176:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 177:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 178:

The Court should disregard the proposed finding because it is contradicted by the evidence cited. (CCRRFF ¶ 173 (addressing substantively identical Proposed Finding 173).

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

Response to Finding No. 179:

Complaint Counsel has no specific response.

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

Response to Finding No. 180:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 181:

The proposed finding is misleading to the extent it suggests Ms. Brown testified her Internet access was blocked through technical means. Ms. Brown testified that she believed that her Internet access was limited to insurance companies' websites, but she did not attempt to access any sites other than insurance companies' websites. (CX0706 (Brown, Dep. at 115-16)).

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)).

Response to Finding No. 182:

Ms. Brown testified that she understood that non-managers did not have the ability to "run" reports. (CX0706 (Brown, Dep. at 114)). She testified that her knowledge of the assignment of differing access levels based on whether a user was a manager was hearsay from another employee. (CX0706 (Brown, Dep. at 113)).

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)).

Response to Finding No. 183:

Complaint Counsel has no specific response.

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

Response to Finding No. 184:

The proposed finding is misleading to the extent it suggests that employees other than Ms. Brown shredded insurance aging reports. Ms. Brown testified that she shredded insurance aging reports. (CX 0706 (Brown, Dep. at 143-44)). However, Ms. Brown worked on-site at LabMD only from May 2005 through May 2006; from May 2006 until leaving LabMD in March 2013, Ms. Brown worked from home and went to the office once per month. (CX0706 (Brown, Dep. at 6-7)). She was not in a position to observe the regular practice of other LabMD employees. And there is contrary evidence that at least [Former LabMD Employee] recycled insurance aging reports. (CCRRFF ¶ 173).

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)).

Response to Finding No. 185:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 186:

The proposed finding is misleading and contradicted by the weight of the evidence. The cited testimony does not provide any details regarding the training Ms. Gilbreth testified she received. (CX0715-A (Gilbreth, Dep. at 77)). And Ms. Gilbreth refers to annual training "at both LabCorp and LabMD." (CX0715-A (Gilbreth, Dep. at 77)). No other LabMD employee

testified to receiving annual training sessions. (*See, e.g.*, CX0714-A ([Former LabMD Employee], Dep. at 87) (one video training at outset of employment); CX0708 (Carmichael, Dep. at 24) (provided compliance training whenever there was a class of new hires). And whatever training LabMD did provide, it did not cover specific measures to safeguard personal information. (CCFF ¶¶ 866-900).

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)).

Response to Finding No. 187:

The proposed finding is misleading to the extent it suggests Ms. Gilbreth provided training on the "security handbook."

Ms. Gilbreth testified that she conducted training for new employees on the employee handbook and "security handbook." (CX0715-A (Gilbreth, Dep. at 81)). She identified the employee handbook as CX0002. (CX0715-A (Gilbreth, Dep. at 82-83)). She testified that she provided the handbook to employees to read, and then highlighted particular areas, "primarily having to do with how the vacation time is laid out, and that using personal e-mail was unacceptable." (CX0715-A (Gilbreth, Dep. at 83)). She did not know any specific measures LabMD took to comply with HIPAA, and did not identify any such measures to new employees. (CX0715-A (Gilbreth, Dep. at 83-84)).

Ms. Gilbreth never identified the "security handbook" to which she referred. She stated that she had some familiarity with CX0006, LabMD's policy manual, but recognized only some of the paragraphs through the first couple pages. (CX0715-A (Gilbreth, Dep. at 84-85)). She did not testify to providing training based on CX0006, LabMD's policy manual, and testified that only "parts of it are familiar" to her. (CX0715-A (Gilbreth, Dep. at 85-86)).

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)).

Response to Finding No. 188:

Complaint Counsel has no specific response.

189. Gilbreth testified the aging reports were shredded. (CX0715-A (Gilbreth, Dep. at 14-16)).

Response to Finding No. 189:

The proposed finding is misleading to the extent it asserts that all billing staff shredded the insurance aging reports. There is contrary evidence that at least [Former LabMD Employee] recycled insurance aging reports. (CCRRFF ¶ 173).

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)).

Response to Finding No. 190:

The proposed finding is misleading to the extent it suggests Ms. Gilbreth testified her Internet access was blocked through technical means throughout the course of her employment.

Ms. Gilbreth testified that some categories of websites were blocked in 2013. (CX0715-A (Gilbreth, Dep. at 64)). She did not have a full recollection as to whether the restrictions were in place for 2012, and stated that her memory started to "get gray" as to whether the restrictions were in place in 2011 and before. (CX0715-A (Gilbreth, Dep. at 64)). Prior to the restrictions going into place, Ms. Gilbreth testified that there were no restrictions on her access to the Internet, and no technical computer restrictions that prevented her from downloading any application that she wanted from the Internet. (CX0715-A (Gilbreth, Dep. at 64-65)).

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)).

Response to Finding No. 191:

The proposed finding is misleading because Ms. Gilbreth testified only regarding one document, CX0006, the LabMD Policy Manual. (CX0715-A (Gilbreth, Dep. at 85-86)). The proposed finding is also misleading to the extent it suggests that a LabMD document titled "IT security handbook" exists. (CX0715-A (Gilbreth, Dep. at 85-86)). Ms. Gilbreth stated that she had some familiarity with CX0006, but recognized only some of the paragraphs through the first couple pages. (CX0715-A (Gilbreth, Dep. at 84-85)). She testified that only "parts of it are familiar" to her. (CX0715-A (Gilbreth, Dep. at 85-86)). She did not specify which parts were familiar, except to say "some of the paragraphs through the first couple of pages," and she did not discuss any data security steps taken in response to the document. (CX0715-A (Gilbreth, Dep. at 84-86)).

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

Response to Finding No. 192:

Ms. Gilbreth testified that she "believe[d]" there was a policy "in general" against the use of personal email accounts. (CX0715-A (Gilbreth, Dep. at 57). She did not recall if there was a requirement that information sent to a personal email account be encrypted. (CX0715-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)).

Response to Finding No. 193:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 194:

The Court should disregard the proposed finding because it merely provides a lay opinion and does not state any fact. Ms. Gilbreth was a finance manager and billing manager, not an IT professional. (CX0715-A (Gilbreth, Dep. at 6, 8, 78)).

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)).

Response to Finding No. 195:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 196:

The Court should disregard the proposed finding as the claim that Mr. Boyle "brought to LabMD an enormous amount of knowledge and experience in information technology and data security" because it is improper expert opinion and is not supported by the citation to the record. Mr. Boyle testified to performing lab work at Cyto Diagnostics, involving slide preparation and slide analysis and supervising the same. (CX0704-A (Boyle, Dep. at 92-96)). Mr. Boyle did not testify to performing any information technology or data security duties at Cyto Diagnostics.

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)).

Response to Finding No. 197:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 198:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 199:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 200:

The proposed finding is misleading to the extent it implies that Mr. Boyle testified that he evaluated or considered data security in choosing and implementing a new billing and laboratory system. (CX0704-A (Boyle, Dep. at 105-109)). Mr. Boyle served as an intermediary between different operating departments and the IT department and did not choose the system on his own: the decision was made by committee, from the top down. (CX0704-A (Boyle, Dep. at 109)). UroCor did not implement the system. (CX0704-A (Boyle, Dep. at 108) .

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)).

Response to Finding No. 201:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 202:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 203:

The proposed finding is misleading to the extent it suggests Mr. Boyle implemented security measures for the transfer of personal information. Mr. Boyle stated that others, not he, had primary responsibility for security. (CX 0704-A (Boyle, Dep. at 115, 117-118)). Mr. Boyle stated that he was aware that security measures were in place, but he did not recall what the tools were. (CX 0704-A (Boyle, Dep. at 117)).

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)).

Response to Finding No. 204:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's process in relation to pre-existing or competing processes. The Court should also disregard the proposed finding because it is impermissible expert testimony.

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)).

Response to Finding No. 205:

The proposed finding is impermissible expert testimony. Upon joining LabMD, Mr. Boyle did not have any data security expertise and his involvement with data security had been minimal. (CCRRFF ¶¶ 196, 200, 202, 203). The Court should also disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's process in relation to pre-existing or competing processes. To the extent it asserts that LabMD's network was secure, the proposed finding is also contradicted by the weight of the evidence regarding the security of LabMD's transfer of information to and from physician clients and internally. (*See, e.g.*, CCFF ¶¶ 4.3.4.3 (The Mapper Server Had Several High Risk Vulnerabilities).

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

Response to Finding No. 206:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. Further, the proposed finding is contradicted by the weight of the evidence. LabMD received Personal Information from physician-clients using the Mapper server. (CCFF ¶¶ 84-90, 220-223). It did not conduct a penetration test on the Mapper server until 2010 (CCFF ¶¶ 715-726, 729-743), even though penetration tests provide a hacker's eye view of network security. (CCFF ¶ 715). The May 2010 penetration test rated the Mapper's security as "poor." (CCFF ¶ 747). The test found more than 30 vulnerabilities in the Mapper server, including high risk vulnerabilities involving the FTP program that LabMD used to transfer information from the offices of physician-clients to the Mapper server. (CCFF ¶¶ 752-797).

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)).

Response to Finding No. 207:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, LabMD did not provide compliance training in data security (CCRRFF ¶ 252 (employees did not receive training in data security)), and did not have technical measures in place to prevent employees from downloading programs or applications from the Internet. (CCFF ¶¶ 1050-1063 (until November 2010, most employees had administrative access to their computers and were able to install programs on them)).

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

Response to Finding No. 208:

Complaint Counsel has no specific response.

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

Response to Finding No. 209:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 210:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 211:

The proposed finding is misleading because it is contradicted by the weight of the evidence. APT did not manage or secure LabMD's internal network or assess risks and vulnerabilities. (CCFF ¶¶ 182-190). Its role was to install computers, connect them to networks, and respond to problems raised by LabMD employees, such as internet connectivity and speed. (CCFF ¶¶ 182-190). In 2006 or 2007, LabMD replaced APT with LabMD employees. (CCFF ¶ 190).

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)).

Response to Finding No. 212:

The proposed finding is misleading to the extent that it suggests that APT performed services for LabMD throughout the Relevant Time Period because it is contradicted by the weight of the evidence. LabMD internally managed its network. (CCFF ¶ 173). In 2006 or 2007, LabMD replaced APT with LabMD employees. (CCFF ¶ 190). When APT was working for LabMD, APT did not manage or secure LabMD's internal network or assess risks and vulnerabilities. (CCFF ¶¶ 182-190). Its role was to install computers, connect them to networks, and respond to problems raised by LabMD employees, such as internet connectivity and speed. (CCFF ¶¶ 182-190).

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)).

Response to Finding No. 213:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 214:

The Court should disregard the proposed finding because it is not supported by the citations to the record. (*See also* CCRRFF ¶ 207 (addressing substantively identical Proposed Finding 207)).

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)).

Response to Finding No. 215:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Furthermore, the proposed finding of fact is misleading to the extent that it suggests that the daily walk arounds involved any data security issues. (CCRRFF ¶¶ 233-235, 251; CCFF ¶¶ 660-685). And LabMD's manual inspections of employee computers for compliance with the policy were haphazard and ineffective. (CCFF ¶¶ 660-687, 691-696).

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)).

Response to Finding No. 216:

The Court should disregard the proposed finding because it is not supported by the citations to the record. The proposed finding is also misleading to the extent it suggests that it relates to data security issues or vulnerabilities. (CCRRFF ¶ 215)). And LabMD's manual inspections of employee computers for compliance with the policy were haphazard and ineffective. (CCFF ¶¶ 660-663, 668-687, 691-696).

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).

Response to Finding No. 217:

To the extent that the proposed finding states that Mr. Wallace testified that he downloaded the 1718 File, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citation to the record and it attempts to state a legal conclusion. That legal conclusion is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs.

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

Response to Finding No. 218:

To the extent that the proposed finding states that Mr. Wallace testified that Tiversa attempted to monetize certain information, Complaint Counsel has no specific response. The Court should otherwise disregard the proposed finding because it is not supported by the citations to the record and it attempts to state a legal conclusion. In particular, none of the citations relates to the 1718 File. In addition, the proposed legal conclusion is unsupported by any legal authority, as required by the Court's Order on Pre-Trial Briefs.

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).

Response to Finding No. 219:

The Court should disregard the proposed finding because it is not supported by citations to the evidentiary record, in violation of the Order on Post-Trial Briefs, attempts to state a legal conclusion, andis irrelevant to this case. Complaint Counsel does not dispute the content of Respondent's quotation. Furthermore, the record does not show that anyone violated this law in connection with Complaint Counsel's investigation or prosecution of this case. (CCRRCL ¶¶ 115-117).

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)).

Response to Finding No. 220:

The Court should disregard the proposed finding because it is not supported by citations to the evidentiary record, in violation of the Order on Post-Trial Briefs, attempts to state a legal conclusion, and is irrelevant to this case. Even if Mr. Wallace had violated the law in obtaining the file, that fact would have no bearing on Complaint Counsel's case, as he did not act at the Commission's direction. (*See* CCRRCL ¶ 115).

218a. "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)).

Response to Finding No. 218a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. The proposed finding is also irrelevant because whether LabMD was regulated by HHS under HIPAA is irrelevant to this case. (*See* CCRRFF ¶¶ 298-99). Furthermore, the FTC's Complaint in this action does not use the term "health care provider" or "HIPAA;" nor does it opine in any way on whether LabMD is subject to HIPAA. Thus, the Complaint cannot "make clear" that LabMD was a health-care provider subject to HIPAA. In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

218b. 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).

Response to Finding No. 218b:

The Court should disregard the proposed finding because it is not supported by citations to the evidentiary record, in violation of the Order on Post-Trial Briefs, attempts to state a legal conclusions, and is irrelevant to this case. Complaint Counsel does not dispute the content of Respondent's quotation. Furthermore, the record does not show that any person violated this law in connection with Complaint Counsel's investigation or prosecution of this case. (CCRRCL ¶¶ 122-125).

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

Response to Finding No. 221:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 222:

Complaint Counsel has no specific response.

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

Response to Finding No. 223:

The proposed finding is misleading because it is ambiguous what Respondent refers to by "this." To the extent that Respondent intended the proposed finding to state that Tiversa's May 2008 communications with LabMD occurred after Tiversa had provided the 1718 File to Dr. Johnson, the Court should disregard the proposed finding because it is not supported by the citation to the record.

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")).

Response to Finding No. 224:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. (*See* CCRRCL ¶¶ 123, 125 (responding to proposed conclusions of law regarding Tiversa's actions related to the 1718 File)). In addition, the Court should disregard the proposed finding because it is not supported by the citation to the record.

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

Response to Finding No. 221a:

The Court should disregard the proposed finding because it is not supported by the citations to the record.

222a. 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)).

Response to Finding No. 222a:

Complaint Counsel has no specific response.

223a. 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)).

Response to Finding No. 223a:

Complaint Counsel has no specific response.

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

Response to Finding No. 224a:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 225:

To the extent the proposed finding indicates that any firewall prohibited employees from going to unspecified websites, the proposed finding is contradicted by the evidence. Ms. Gilbreth testified that prior to approximately 2010 there were no restrictions on her access to the Internet, and no technical computer restrictions that prevented her from downloading any application that she wanted from the Internet. (CX0715-A (Gilbreth, Dep. at 64-65); *see also* CX0730 (Simmons, Dep. at 125-26 (expressing belief that restrictions did not apply to lab technicians)). Other employees testified that while they believed their Internet access was limited to insurance companies' websites, they did not attempt to access non-permitted websites and did not know if technical restrictions would have prevented them from doing so. (CX0716 (Harris, Dep. at 82-83) (employed October 2006 through January 2013, *id.* at 10-11); CX0706 (Brown, Dep. at 115-16) (employed May 2005 through May 2006 on site, and then May 2006 through March 2013 remotely, *id.* at 6-7)). Furthermore, Ms. Simmons did not have knowledge of security provided by LabMD's firewall. She testified that "I think there was a firewall protecting our network, but I never dealt with that part of it." (CX0734 (Simmons, IHT at 21)).

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)).

Response to Finding No. 226:

The Court should disregard the proposed citation because it is not supported by the citation to the record as to Mr. Martin's participation in a search of computers that contained either LimeWire or the 1718 File at LabMD's direction. (CX0704-A (Boyle, Dep. at 61-63)).

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)).

Response to Finding No. 227:

The proposed finding is misleading to the extent it indicates that Ms. Simmons's search was exhaustive. Ms. Simmons testified to searching by filename. (CX0730 (Simmons, Dep. at 17-18)). She did not testify to searching by file extension, hash, or using a browse host function. (CCFF ¶¶ 1269-70 (describing hash searching), ¶¶ 1284-1288 (describing file extension searching), ¶¶ 1291-1296 (describing host browsing)). Furthermore, searches may sometimes fail to find files that are on the Gnutella network because searches only cover a portion of the network, due to high use, network congestion, and the limited number of "hops" a request will be forwarded, or if the computer on which the file is located is not connected to the Internet or running a file-sharing application. (CCFF ¶¶ 1250-1251, 1259-1266).

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)).

Response to Finding No. 228:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 229:

The proposed finding is misleading to the extent it indicates that Ms. Simmons's and Mr. Martin's searches were exhaustive. The cited testimony does not describe the means by which Ms. Simmons and Mr. Martin searched the P2P network. (*See* CCRRFF ¶ 227)). In addition, the proposed finding is misleading to the extent it implies that because Ms. Simmons and Mr. Martin did not find the file, it had not been accessed and/or was not still or later available on P2P networks. (*See* CCFF ¶¶ 1250-1251, 1259-1266).

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)).

Response to Finding No. 230:

Complaint Counsel has no specific response.

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

Response to Finding No. 231:

Complaint Counsel does not dispute that LabMD had this policy. However, LabMD failed to enforce this policy. (CCFF ¶¶ 458-462).

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

Response to Finding No. 232:

To the extent it implies that Ms. Woodson was terminated because of the P2P incident, the proposed finding is contradicted by the weight of the evidence. The evidence shows that she was fired for poor performance as well as the P2P incident. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 11, Resp. to Interrog. 19; CX0704-A (Boyle, Dep. at 156); CX0736 (Daugherty, IHT at 91)). This is further supported by the fact that she was not terminated until two months after the incident, on July 31, 2008. (CX0681 (Rosalind Woodson Dates of Employment) at 7).

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)).

Response to Finding No. 233:

The Court should disregard the proposed finding because it is not supported by the citations to the record.

Furthermore, from March 2004 through at least October 2009, LabMD did not inspect employee desktops for security issues on a regular basis; rather, LabMD IT employees inspected employee workstations only if the employee requested it because the computer was not functioning properly. (CCFF ¶¶ 668-677). Mr. Bureau testified that he did not proactively review employee workstations on a regular basis. (CX0707 (Bureau, Dep. at 50-52, 89-90)). Mr. Hyer did not have a formal practice to manually inspect desktop computers, and testified that nobody else at LabMD conducted regular manual inspections of desktop computers with him. (CX0719 (Hyer, Dep. at 95-96, 99)).

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)).

Response to Finding No. 234:

The Court should disregard the proposed finding because it is not supported by the citations to the record. As Respondent's citations demonstrate, from March 2004 through at least October 2009, LabMD did not inspect employee desktops for security issues on a regular basis; rather, LabMD IT employees inspected employee workstations only if the employee requested it because the computer was not functioning properly. (CCFF ¶¶ 668-677). Mr. Hyer, who was employed at LabMD from August 2009 to September 2011, testified that he performed manual inspections not more than once a week, did not have a formal practice when he did so, and that nobody else at LabMD performed manual inspections while he was there. (CX0719 (Hyer, Dep. at 95-96, 99); CCFF ¶¶ 344-347). The cited exhibits do not reflect daily security checks; rather, consistent with employee testimony regarding walkarounds described above, they reflect troubleshooting and functioning of computers, rather than security. (*See, e.g.*, RX179 (noting need to replace toner cartridges and an employee computer not networked properly), RX182 (discussing printer functioning and forms in Lytec), RX186 (noting installation of memory in computer), RX189 (noting need to replace toner cartridges), RX191 (discussing shelves and white board); CX0199 (noting printer is ready for pickup)).

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)).

Response to Finding No. 235:

The Court should disregard the proposed finding because it is not supported by the citations to the record.

Furthermore, through at least October 2009, LabMD did not physically or manually inspect employee desktops for security issues on a regular basis; rather, LabMD IT employees inspected employee workstations only if the employee requested it because the computer was not functioning properly. (CCFF ¶¶ 668-677). From August 2009 through September 2011, employee desktops were reviewed no more than once a week, and no formal checklist was used. (CCRRFF ¶ 234; CX0719 (Hyer, Dep. at 98)).

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)).

Response to Finding No. 236:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Boyle testified at the cited page only that Mr. Hyer was hired to control network security. (CX0704-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)).

Response to Finding No. 237:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 238:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 239:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Hyer does not address Mr. Kaloustian's qualifications. (*See* CX0719 (Hyer, Dep. at 41-42)). To the extent Mr. Hyer testified about Mr. Kaloustian's abilities, his statements are vague and conclusory, and do not support any factual inferences. (CX0719 (Hyer, Dep. at 41-42)). Notwithstanding, Complaint Counsel relies on the testimony of Mr. Kaloustian only to establish facts of which he has personal knowledge, not for best practices.

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

Response to Finding No. 240:

The Court should disregard the proposed finding because it is not supported by the citations to the record. To the extent it asserts that LabMD was using TrendMicro or Symantec for all computers since 2005, the proposed finding is also contradicted by the weight of the evidence. First, LabMD used the ClamWin and AVG antivirus programs on employee computers from at least October 2005 until late 2009 (CCRRFF ¶ 150, CCFF ¶ 566-567, 581-584, 615; RFF ¶ 151), not Trend Micro. Second, LabMD installed ClamWin antivirus software on computers provided to its physician clients. (RFF ¶¶ 151, 259).

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)).

Response to Finding No. 241:

Complaint Counsel has no specific response.

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

Response to Finding No. 242:

The proposed finding is ambiguous as to "the system." In addition, the proposed finding is not supported by the citation to the record as to the time period before and after Mr. Hyer's tenure. *See* Scheduling Order, Additional Provisions ¶ 17 (Sept. 25, 2013) (personal knowledge showing required). Otherwise, Complaint Counsel has no specific response.

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

Response to Finding No. 243:

To the extent the proposed finding asserts that LabMD had TrendMicro installed on all of its network, it is contradicted by the weight of the evidence. (CCRRFF ¶ 240; CCFF ¶¶ 539-563 (Symantec used on servers); *see also* RFF ¶ 240 (Symantec also used), ¶ 151 (ClamWin used on client computers)). To the extent the proposed finding purports to apply from 2005 to the present, it should be disregarded because Mr. Boyle does not have personal knowledge to cover the entire time period. *See* Scheduling Order, Additional Provisions ¶ 17 (Sept. 25, 2013) (personal knowledge showing required). To the extent the proposed finding asserts that LabMD staff were reviewing TrendMicro reports from 2005 to the present, it is contradicted by the weight of the evidence, because the evidence shows that many LabMD computers were not using TrendMicro during the Relevant Time Period. (CCRRFF ¶ 240). To the extent the proposed finding asserts that TrendMicro software has the capability to create a report that can be reviewed, Complaint Counsel has no specific response.

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

Response to Finding No. 244:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Mr. Boyle only testifies at the cited location that software other than

TrendMicro was in use for servers and work stations, but he did not remember what other antivirus software was used. (CX0704-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)).

Response to Finding No. 245:

The proposed finding does not describe how firewalls, routers, and Websense protected LabMD's network. Furthermore, the evidence shows that LabMD's firewall applications were deployed haphazardly or not at all and were not properly configured. (CCFF ¶¶ 631-657, 1075-1105). LabMD's routers did not have logging capability (CCFF ¶ 246), were not tested for vulnerabilities (CCFF ¶¶ 178-179), and LabMD had no written policy to update the software of its routers. (CCFF ¶ 1043). LabMD's router was not configured to provide firewall protection at its Powers Ferry Road location. (CCFF ¶ 1086).

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)).

Response to Finding No. 246:

The proposed finding is contradicted by the weight of the evidence. LabMD did not have written policies requiring password complexity, password reuse, and other reasonable password creation practices (CCFF ¶¶ 919-930, 954-957), and LabMD did not enforce the password policies it had, such as by assessing the strength of employee passwords (CCFF ¶¶ 941-942), or requiring employees to change from the default password they were assigned (CCFF ¶ 930).

The proposed finding is also misleading to the extent it suggests LabMD otherwise restricted the information employees could access. LabMD did not implement access controls to prevent employees from accessing sensitive information they did not need to perform their jobs. (CCFF ¶¶ 811-827).

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)).

Response to Finding No. 247:

To the extent the proposed finding asserts that LabMD retained ProviDyn in May 2010, Complaint Counsel has no specific response. To the extent it asserts that LabMD retained Providyn to conduct quarterly scans, the Court should disregard it because it is not supported by the citations to the record. On the contrary, neither CX0044 or Mr. Boyle's testimony indicate quarterly scans. (CX0044 (Providyn Service Solutions Proposal for LabMD, executed by M. Daugherty); CX0704-A (Boyle, Dep. at 34-41)). In fact, the record reflects that only three sets of scans of LabMD's servers and network were conducted by ProviDyn (CX0066 – CX0074, CX0077 – CX0084 (May 21, 2010), CX0054 – CX0055 (July 18, 2010), CX0057 – CX0065 (September 3, 2010)).

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)).

Response to Finding No. 248:

The Court should disregard the proposed finding because it is not supported by the citations to the record. In the cited testimony, Mr. Hyer states only that a level 5 risk is a "critical risk" that "needs to be addressed right away" and said he was "sure that [he] reviewed it, resolved it," but did not provide any details. (CX 0719 (Hyer, Dep. at 108-10)). The cited testimony does not indicate that risks were actually addressed. LabMD did not resolve all the critical risk items on the ProviDyn vulnerability scan assessments. (CX0704-A (Boyle, Dep. at 37) (stating that while a resolution was defined for each vulnerability identified by ProviDyn, the resolution was not always put into place to resolve the vulnerability)).

In fact, the July 18 and September 3 ProviDyn scans revealed that vulnerabilities identified in the May 21 scan were still present. (CCFF ¶ 757 (port 21 open in all three scans, providing access to Microsoft FTP program running on Mapper server), ¶¶ 759-771 (Level 5 Anonymous FTP Writeable root Directory vulnerability, which could allow export of all the data on the Mapper server, found in May and July scans), ¶¶ 781-788 (Anonymous FTP Enabled vulnerability, which allowed a remote user without any access credentials to access any files made available on the FTP server, present on Mapper server in May and July scans), ¶¶ 792-797 (FTP Supports Clear Text Authentication vulnerability, which made usernames and passwords for the FTP application on Mapper vulnerable to sniffing by transmitting them in clear text, present on Mapper server in all three scans), ¶¶ 800-808 (Port 3306 found open in May and July scans, making vulnerable the database application LabMD used to store sensitive consumer information)).

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)).

Response to Finding No. 249:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The risk assessment levels in the ProviDyn reports are based on international and recognized security standards, including the PCI Security Standard and the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards (NIST). (CCFF ¶ 737). A vulnerability's threat-likelihood rating takes into account factors such as the ease or difficulty of exploiting the vulnerability and the impact on confidentiality, integrity, and/or availability. (CCFF ¶¶ 499-509; *see*, *e.g.*, CX0740 (Hill Report) at 63) (citing National Vulnerability Database, *available at* http://web.nvd.nist.gov/view/vuln/

detail?vulnId=CVE-1999-0527). Mr. Hyer's testimony does not indicate an expertise equal to or exceeding these sources.

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)).

Response to Finding No. 250:

The proposed finding is not supported by citation to the record. Mr. Hyer testified that he was not aware of any data security breaches during his tenure. (CX0719 (Hyer, Dep. at 156-57)). Moreover, he does not state anything regarding "point to point information being transferred between LabMD and its physician clients," or state that he would be aware of such a breach if it occurred. (CX0719 (Hyer, Dep. at 156-57)).

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)).

Response to Finding No. 251:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, LabMD IT employees testified that they did not use the Walkaround Checklist, CX0482. (CX0730 (Simmons, Dep. at 143); CX0719 (Hyer, Dep. at 98)).

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)).

Response to Finding No. 252:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Mr. Boyle states only that LabMD created new security procedures that included "training discussions." (CX0704-A (Boyle, Dep. at 68)).

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

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

Response to Finding No. 253:

Complaint Counsel has no specific response.

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

Response to Finding No. 254:

The proposed finding is misleading to the extent it implies that Mr. Maire had expertise in information security. Mr. Maire took a single wireless security class in pursuit of his degree, and did not study any other security aspects of information technology. (CX0724 (Maire, Dep. at 8-9)).

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)).

Response to Finding No. 255:

The proposed fact is misleading to the extent that it suggests Mr. Maire testified that LabMD had written information security policies. The only information security-related policy he testified to seeing in writing was a prohibition on use of LabMD equipment for "personal use or nonauthorized [sic] LabMD operations." (CX0724 (Maire, Dep. at 18-19)). Mr. Maire could not recall if any security topics were covered under the "HIPAA guidelines and regulations we were to follow" he mentioned. (CX0724 (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)).

Response to Finding No. 256:

The proposed fact is misleading to the extent it suggests that Mr. Maire performed any security-related checks during his rounds. Mr. Maire's daily IT rounds involved "visit[ing] each section to query the endusers [sic] if they had an issue with any of their personal machines or a peripheral that was not known." (CX0724 (Maire, Dep. at 46)). If Mr. Maire was informed by a user that there was no issue with the operation of their computer, he would move on to the next user. (CX0724 (Maire, Dep. at 48)).

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)).

Response to Finding No. 257:

The proposed finding is misleading to the extent it indicates that CX0006 was a written document during Mr. Maire's tenure of May 2007 through June 2008. LabMD's Policy Manual (CX0006) did not exist in writing until 2010 (JX0001-A (Joint Stips. of Law, Fact, and

Authenticity) at 4, Stip. 6), and Mr. Maire testified that he only saw the Policy Manual as a full document after being provided it by Respondent's counsel. (CX0724 (Maire, Dep. at 20)).

The proposed finding is further misleading to the extent it suggests the citation supports an inference that Mr. Maire participated in implementing or enforcing these policies, or that he had any knowledge that they were implemented or enforced. Mr. Maire's role in implementing or enforcing these policies was limited to ensuring that all computers had TrendMicro installed on them. (CX0724 (Maire, Dep. at 22)). While Mr. Maire testified that he had "a role" in enforcing the monitoring of security software settings and applying operating system updates (CX0724 (Maire, Dep. at 24)), his testimony regarding manual inspections indicates that they were performed only to troubleshoot operating issues, not to address data security vulnerabilities, and only at request of the user, not on the monthly basis indicated by the Policy Manual. (CX0006 (Policy Manual) at 13; CCRRFF ¶ 256)).

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

Response to Finding No. 258:

The proposed finding is misleading to the extent it suggests a firewall is an "intrusion prevention system," or that LabMD's firewall operated as such. (CCRRFF ¶¶ 155 (addressing identical Proposed Finding 155)).

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

Response to Finding No. 259:

Complaint Counsel has no specific response.

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

Response to Finding No. 260:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 261:

The proposed finding is misleading to the extent it suggests Mr. Maire would be aware of any breach or unauthorized access to information. Mr. Maire did not have data security responsibilities at LabMD. (CCRRFF ¶ 154)). The proposed finding is also misleading to the extent it suggests Mr. Maire was not aware of the sharing of the 1718 File on a P2P network. (CX0724 (Maire, Dep. at 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)).

Response to Finding No. 262:

The Court should disregard the proposed finding because it is not supported by the citations to the record. The fact that LabMD's Compliance Program document states that "LabMD has the intent is [sic] to be fully compliant with the rules, laws and guidelines regulating its business" does not establish that it took steps to do so. (*See* CX0005 (LabMD Compliance Program) at 1). Likewise, just because the Compliance Program states that LabMD's Compliance Officer "shall implement . . . a formal training program dealing with compliance," including training on "at least an annual basis," does not prove that such training took place. (CX0005 (LabMD Compliance Program) at 9). The only evidence of training is of one-session Compliance Trainings LabMD provided to new employees. (CX0708 (Carmichael,

Dep. at 24, 27, 33, 62, 64). This training informed—not instructed—employees of LabMD's obligations under HIPAA, amongst a host of other laws, but provided no detail on specific information security requirements or LabMD's information security practices. (CX0708 (Carmichael, Dep. at 25-26, 28-29, 42, 46-47, 55-56, 58-60); *see* CX0127 (LabMD Compliance Training)). Furthermore, LabMD did not provide the additional job-specific training required by its Compliance Program. (CX0718 (Hudson, Dep. at 70-73, 137, 139); CX0005 (LabMD Compliance Program) at 9).

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)).

Response to Finding No. 263:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 264:

The proposed finding is misleading to the extent it implies that LabMD provided instruction on compliance with HIPAA's Security Rule, Privacy Rule, and "extant protections for PHI." In fact, LabMD's Compliance Training merely informed employees that they and LabMD had obligations related to security and PHI, but did not provide detail on what they were or how LabMD complied with such requirements. (CX0708 (Carmichael, Dep. at 25-26, 28-29, 42, 46-47, 55-56, 58-60); *see* CX0127 (LabMD Compliance Training)). Furthermore, LabMD did not provide the additional job-specific training required by its Compliance Program. (CX0718 (Hudson, Dep. at 70-73, 137, 139); CX0005 (LabMD Compliance Program) at 9).

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

Response to Finding No. 265:

To the extent the proposed finding is a quotation of an attorney question from Ms. Carmichael's deposition, Complaint Counsel has no specific response. However, the proposed finding is misleading to the extent it implies that, because LabMD's Compliance Program required it to perform regular training related to security, it did so. In fact, the only evidence of training is of one-session Compliance Trainings LabMD provided to new employees. (CX0708 (Carmichael, Dep. at 24, 27, 33, 62, 64). This training informed—not instructed—employees of LabMD's obligations under HIPAA, amongst a host of other laws, but provided no detail on specific information security requirements or LabMD's information security practices. (CX0708 (Carmichael, Dep. at 25-26, 28-29, 42, 46-47, 55-56, 58-60); *see* CX0127 (LabMD Compliance Training)). Furthermore, LabMD did not provide the additional job-specific training required by its Compliance Program. (CX0718 (Hudson, Dep. at 70-73, 137, 139); CX0005 (LabMD Compliance Program) at 9).

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)).

Response to Finding No. 266:

The Court should disregard the proposed finding because it is not supported by the citations to the record. The cited exhibits were not referenced or discussed by any witness to shed light on their meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). They cannot speak for themselves. To the extent any information can be deduced from the exhibits, they do not support the proposed finding's assertion that

"daily" scans were run during the period June 2010 – July 2010, or the broader proposition that LabMD ran virus scans on its systems throughout the Relevant Time Period. Most of the chart on RX266 contains a single date, "6/11/2010," and where multiple date entries appear the maximum number is four and the dates are not sequential. Likewise, most of the chart on RX267 contains a single date, "7/5/2010," and where multiple date entries appear the maximum number is four and the dates are not sequential.

Furthermore, the proposed finding does not provide any information regarding the reasonableness of the virus scans, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, whether the virus definitions had been updated, or any other relevant information.

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)).

Response to Finding No. 267:

The Court should disregard the proposed finding because it is not supported by the citations to the record. The cited exhibits were not referenced or discussed by any witness to shed light on their meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). The exhibits cannot speak for themselves, (*see* CCRRFF ¶ 266), and do not even contain the term "RealTime Scanning." To the extent any information can be deduced from the exhibits, they do not support the proposed finding with regard to the period June 2010 – July 2010, or the broader proposition that RealTime Scanning was active on LabMD's systems throughout the Relevant Time Period, because the exhibits only state a handful of dates. (*See* CCRRFF ¶ 266).

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)).

Response to Finding No. 268:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). It cannot speak for itself. (*See* CCRRFF ¶ 266).

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)).

Response to Finding No. 269:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). It cannot speak for itself. (*See* CCRRFF ¶ 266).

Furthermore, the proposed finding does not provide any information regarding the function or reasonableness of Regular Cleaner, TrendMicro, and Security Check software, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, or any other relevant information.

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)).

Response to Finding No. 270:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). It cannot speak for itself. (*See* CCRRFF ¶ 266)). To the extent any information can be deduced from the exhibit, it does not support the proposed finding that LabMD used Malwarebytes software on its systems throughout the Relevant Time Period, because the exhibit only states a handful of dates. (*See* CCRRFF ¶ 266).

Furthermore, the proposed finding does not provide any information regarding the function or reasonableness of Malwarebytes software, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, or any other relevant information.

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)).

Response to Finding No. 271:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8). It cannot speak for itself. (*See* CCRRFF ¶ 266)).

To the extent any information can be deduced from the exhibit, it does not support the proposed finding that LabMD used Regular Cleaner and Security Check software on its systems

throughout the Relevant Time Period, because the exhibit only lists a single date in the columns related to these software programs. (*See* CCRRFF ¶ 266).

Furthermore, the proposed finding does not provide any information regarding the function or reasonableness of Regular Cleaner and Security Check software, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, or any other relevant information.

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)).

Response to Finding No. 272:

The cited exhibit does not support the proposed finding on its face. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8).

273. In addition, to the extent the proposed finding asserts that LabMD used TrendMicro on all its systems and throughout the Relevant Time Period, it is not supported by the cited exhibit, which appears to indicate two dates under the TrendMicro column, and is contradicted by the weight of the evidence. (CCRRFF ¶¶ 240, 243).Furthermore, the proposed finding does not provide any information regarding the function or reasonableness of TrendMicro, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, or any other relevant information. 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)).

Response to Finding No. 273:

The cited exhibit does not support the proposed finding on its face. The cited exhibit was not referenced or discussed by any witness to shed light on its meaning. (Resp't's Proposed Findings of Fact Attachment 1, at 8 (Resp't Counsel's Exhibit Index at 8).

To the extent any information can be deduced from the exhibit, it does not support the proposed finding that LabMD used Malwarebytes software on the stated servers on the stated dates, or the broader finding that it used Malwarebytes software on its systems throughout the Relevant Time Period, because the exhibit only states a handful of dates. (*See* CCRRFF ¶ 266).

Furthermore, the proposed finding does not provide any information regarding the function or reasonableness of Malwarebytes, any data security problems or vulnerabilities identified, whether LabMD acted on such problems or vulnerabilities, or any other relevant information.

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)).

Response to Finding No. 274:

To the extent the proposed finding asserts that Mr. Fisk is an expert on data security, it is misleading. (CCRRFF ¶ 275). To the extent it only recites the Relevant Time as Mr. Fisk defined it, Complaint Counsel has no specific response.

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)).

Response to Finding No. 275:

The proposed finding is misleading to the extent that it suggests that Mr. Fisk has meaningful experience with "security." While Mr. Fisk has substantial experience designing P2P software, Respondent has presented no evidence that he has any experience that would allow him to evaluate the overall security posture of businesses' computer networks. Mr. Fisk's experience is devoted solely to the development of P2P software. (*See* RX533 (Fisk Report) at

35 (describing Mr. Fisk's experience from 2000 to the present); Fisk, Tr. 1175-1177 (admitting that he testified at his deposition that he had never evaluated a company's data security)).

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

Response to Finding No. 276:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 277:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 278:

The proposed finding is incorrect to the extent that it suggests that Mr. Fisk possesses expertise in "computer networking, and data security." While Mr. Fisk has substantial experience designing P2P software, Respondent has presented no evidence that he has any experience that would allow him to evaluate the overall security posture of businesses' computer networks. Mr. Fisk's experience is devoted solely to the development of P2P software. (*See* RX533 (Fisk Report) at 35 (describing Mr. Fisk's experience from 2000 to the present); Fisk, Tr. 1175-77 (admitting that he testified at his deposition that he had never evaluated a company's data security)).

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

Response to Finding No. 279:

Complaint Counsel agrees that Mr. Fisk's report states that LabMD "adhere[d] to reasonable standards to secure the Protected Health Information it possessed." (RX533 (Fisk Report) at 32). The finding is incorrect, however, to the extent it suggests that this statement is accurate. LabMD did not take reasonable steps to secure personal information in its possession. (*See* CCFF ¶¶ 382-1110).

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)).

Response to Finding No. 280:

The proposed is incorrect both because the standards it suggests as best practices are insufficient to reasonably protect personal information on LabMD's network and because LabMD did not comply with even those standards. The suggestion that best data security practices for a company that handled personal information on the scale that LabMD did are met by merely having firewalls and profiles that prevented non-managers from downloading files and installing apps is contradicted by the weight of the evidence. (*See* CCFF ¶¶ 384-395, 524; CCCL ¶¶ 15-20).

Regardless, LabMD failed to meet even the minimal standards suggested in this finding. First, there is no evidence to support Mr. Fisk's assertion that LabMD had two layers of properly configured firewalls. Mr. Fisk bases his assertion on the fact that the router used by LabMD had firewall capabilities and his assumption that those capabilities were probably turned on. (RX533 (Fisk Report) at 20-21). In fact, the router's firewall capabilities were not activated. (*See* CCFF ¶ 1086). To the extent that Respondent is citing to Mr. Fisk's opinion to establish the fact that the router's firewall capabilities were activated, the finding is also in violation of the Court's

Order on Post-Trial Briefs because it cites an opinion by Respondent's expert to support factual propositions that should be established by fact witnesses or documents.

Mr. Fisk's assertion that LabMD's firewalls were properly configured is equally erroneous. LabMD did not properly configure its firewall to block IP addresses and unnecessary ports. (CCFF ¶¶ 1094-1105).

In addition, LabMD did not, as Mr. Fisk suggests, properly employ profiles that prevented non-managers from downloading files or installing apps. (CCFF ¶¶ 460-462, 1056-1060). Until at least 2009, many LabMD employees had administrative rights to their computers and unrestricted access to the internet. (CCFF ¶¶ 460-462, 1056-1060).

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)).

Response to Finding No. 281:

The proposed finding is misleading to the extent that it suggests that LabMD activated the "firewall and intrusion capabilities" of its router. The router's firewall and intrusion capabilities were not activated. (*See* CCFF ¶ 1086). To the extent that Respondent is citing to Mr. Fisk's opinion to establish the fact that LabMD's router's firewall and intrusion prevention capabilities were activated, the finding also is in violation of the Court's Order on Post-Trial Briefs because it cites an opinion by Respondent's expert to support factual propositions that should be established by fact witnesses or documents.

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)).

Response to Finding No. 282:

The proposed finding is misleading to the extent that it suggests that LabMD had activated the "firewall and intrusion capabilities" of its router, making the ZyWall firewall

"redundant." There is no evidence to support this claim. (*See* CCFF ¶ 1086). To the extent that Respondent is citing to Mr. Fisk's opinion to establish the fact that LabMD's router's firewall and intrusion prevention capabilities were activated, the finding also is in violation of the Court's Order on Post-Trial Briefs because it cites an opinion by Respondent's expert to support factual propositions that should be established by fact witnesses or documents.

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)).

Response to Finding No. 283:

Complaint Counsel agrees that LabMD did not deploy file integrity monitoring, but the proposed finding is misleading to the extent that it suggests that LabMD's manual examinations of employee workstations effectively compensated for LabMD's failure to deploy file integrity monitoring. (*See* CCFF ¶¶ 660-664 (manual inspections could not reliably detect security risks), ¶¶ 668-677 (LabMD performed manual inspections only on request when employee workstations malfunctioned), ¶¶ 680-685 (LabMD did not provide guidance for manual inspections until 2010), ¶¶ 691-696 (LabMD's manual inspections did not detect Limewire), ¶ 708 (manual inspections are less effective and less efficient than file integrity monitoring)).

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

Response to Finding No. 284:

The proposed finding misrepresents Mr. Fisk's report. He did not state that "[t]he best practices guidelines during the Relevant Period did not include File Integrity Monitoring in their recommendations." Instead, he stated that file integrity monitoring was not included in the "best practices guidelines reviewed for this report." (RX533 (Fisk Report) at 33). Mr. Fisk's limited

expertise in information security is not sufficient to determine the relevant best practices at the time. (CCRRFF ¶¶ 275, 278). In any event, these documents cannot support a claim that – for a business maintaining hundreds of thousands of consumers' sensitive personal information, including health information – file integrity monitoring could not be a component of reasonable data security practices.

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)).

Response to Finding No. 285:

The proposed finding is incorrect to the extent it suggests that the 1718 file was not obtained from LabMD through its firewall or that LabMD's firewall prevented the removal of the file. LimeWire permits users to obtain documents from computers that are behind a firewall using an outbound connection to an ultrapeer, so the presence of a firewall on LabMD's system did nothing to prevent the removal of the 1718 file. (*See* CCFF ¶¶ 1234-1237).

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

Response to Finding No. 286:

The proposed finding is incorrect. LabMD's firewall was not properly configured. (CCFF ¶¶ 1094-1105).

286a. 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)).

Response to Finding No. 286a:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 287:

The proposed finding is irrelevant, as Complaint Counsel has not relied upon this portion of Dr. Hill's report. Dr. Hill acknowledged this issue in her rebuttal report and explained that this did not affect her overall opinion about the reasonableness of LabMD's security practices. (CX0737 (Hill Rebuttal Report) ¶¶ 12-13).

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)).

Response to Finding No. 288:

The proposed finding is irrelevant, as Complaint Counsel has not relied upon this portion of Dr. Hill's report. Dr. Hill acknowledged this issue in her rebuttal report and explained that this did not affect her overall opinion about the reasonableness of LabMD's security practices. (CX0737 (Hill Rebuttal Report) ¶¶ 12-13). In addition, the proposed finding is misleading to the extent that it suggests that LabMD's firewall was configured properly. LabMD's firewall was not properly configured. (CCFF ¶¶ 1094-1105).

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)).

Response to Finding No. 289:

The proposed finding is misleading and incomplete. Complaint Counsel agrees that Day Sheets were found on October 5, 2012. (CCFF ¶ 1413). The proposed finding, however, is misleading and incomplete because the Sacramento Police Department (SPD) found, in addition to more than 35 Day Sheets, also 9 copied checks and one money order made payable to LabMD in a house in Sacramento, California. (CCFF ¶ 1413).

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)).

Response to Finding No. 290:

The Court should disregard the proposed finding because it calls for a legal conclusion, not a fact. The Court should also disregard the proposed finding because it is not supported by the citations to the record.

Further, proof of a data breach is not a requirement for Respondent's practices to be unfair in violation of Section 5. (*See* CCCL ¶ 24; CCRRCL ¶ 77).

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

Response to Finding No. 291:

The proposed finding is misleading and incomplete to the extent it suggests that LabMD Day Sheets existed only in paper form. Complaint Counsel agrees that the Sacramento Police Department (SPD) found more than 35 LabMD Day Sheets in paper form at a house in Sacramento, California in the possession of individuals unrelated to LabMD's business who later pleaded no contest to state charges of identity theft. (CCFF ¶¶ 1413-1414.) Although Day Sheets were created, accessed, and printed electronically through LabMD's billing application, Lytec, to ensure payment was received and posted, LabMD's billing employees also had the option of saving Day Sheets electronically to a computer. (CCFF ¶¶ 151, 156). LabMD also scanned and saved some Day Sheets to its computer network as part an archive project by the company. (CCFF ¶ 161).

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)).

Response to Finding No. 292:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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

Response to Finding No. 293:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 294:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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)).

Response to Finding No. 295:

The Court should disregard the proposed finding because it calls for a legal conclusion, not a fact.

Further, Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury. The inquiry turns on whether any potential or actual unauthorized disclosure of Personal Information held by a

company due to unreasonable data security practices caused or is likely to cause consumer harm. (*See* CCCL ¶ 25). Likelihood of harm satisfies the unfairness analysis. (*See* CCCL ¶ 26).

The unauthorized disclosure of the Sacramento Day Sheets and copied checks caused or is likely to cause substantial injury to consumers. (CCFF ¶¶ 1714-1719, 1722-1733, 1736-1739, 1742-1746, 1749-1753, 1756-1760). The Day Sheets and copied checks contain sensitive Personal Information, including first names and last names, middle initials, and Social Security numbers for approximately 600 consumers, and bank routing and account numbers for consumers whose checks are included. (CCFF ¶¶ 1714-1717, 1723). These types of information can be used by identity thieves to commit identity theft resulting in monetary and other harms to affected consumers. (CCFF ¶ 1487-1493). Because consumers rarely change their Social Security numbers, they can be fraudulently used for extended periods of time, making it likely that consumers will suffer injury. (CCFF ¶¶ 1570-1575). The fact that the Day Sheets and copied checks were found, with other evidence of identity theft, in the possession of known identity thieves speaks to the value of the consumer information in the documents and the likelihood that it may have been misused. (CCFF ¶¶ 1413-1414, 1727-1729).

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])).

Response to Finding No. 296:

Complaint Counsel does not dispute that LabMD sent notice letters to the consumers whose sensitive personal information was included in the Day Sheets. (CCFF ¶ 1461). The Court should disregard the remainder of the proposed finding because it provides an opinion and does not state any fact.

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

Response to Finding No. 297:

The proposed finding mischaracterizes Dr. Hill's testimony. On the contrary, Dr. Hill testified as follows:

> Q. And, in fact, it's your opinion that LabMD's physical security was adequate; is that correct?
> A. **Yes. As far as providing locks to server rooms and access to their – physical access to their computers, yes. But physical security is not sufficient in protecting against electronic attacks.**

(Hill, Tr. 293) (emphasis added). As demonstrated by Dr. Hill's full response, Dr. Hill restricted her answer about LabMD's physical security to LabMD's provision of locks to server rooms and physical access to LabMD computers.

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)).

Response to Finding No. 298:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. Whether LabMD was regulated by HHS under HIPAA is irrelevant to this case because LabMD must still comply with the FTC Act. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't's Motion for Summ. Decision at 5-6 (May 19, 2014).

Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

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)).

Response to Finding No. 299:

The FTC has not accused LabMD of violating HIPAA or HITECH. In any event, whether HHS or FTC has accused LabMD of violating these statutes is irrelevant to this case because LabMD must still comply with the FTC Act. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."). Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")). In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

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)).

Response to Finding No. 300:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. In addition, the proposed finding is incorrect. The FTC's Complaint in this action does not use the term "health care provider" or "HIPAA;" nor does it opine in any way on whether LabMD is subject to HIPAA. Thus, the FTC's Complaint cannot "make clear" that LabMD was a health-care provider subject to HIPAA.

In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

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)).

Response to Finding No. 301:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. The proposed finding is also irrelevant. Complaint Counsel agrees that the FTC has not alleged that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing these statutes. However, whether HHS or FTC has accused LabMD of violating these statutes or regulations is irrelevant to this case because LabMD must still comply with the FTC Act. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and

noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't's Motion for Summ. Decision at 5-6 (May 19, 2014).

In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding..

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)).

Response to Finding No. 302:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. The proposed finding is also irrelevant, as Respondent's compliance with HIPAA or HITECH, or lack thereof, is immaterial to this proceeding. Comm'n Order Denying Resp't's Mot. to Dismiss at 10-13 (Jan. 16, 2014); Comm'n Order Denying Resp't's Motion for Summ. Decision at 5-6 (May 19, 2014). Indeed, Respondent has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

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).

Response to Finding No. 303:

The proposed finding is irrelevant. Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding. Regardless, Respondent's compliance with HHS rules and regulations, or lack thereof, is irrelevant to this proceeding. Comm'n Order Denying Resp't's Motion for Summ. Decision at 5-6 (May 19, 2014); Comm'n Order Denying Resp't's Mot. to Dismiss at 10-13 (Jan. 16, 2014). Indeed, Respondent has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

H. The Commission Lacks Standards For Medical Companies

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)).

Response to Finding No. 304:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 305:

The proposed finding is misleading to the extent that it suggests that information produced about data security was not sufficient to inform all entities, including HIPAA-covered entities such as LabMD, of what was expected of them to comply with Section 5. For example, the Commission voted to issue more than 20 complaints charging deficient data security as unfair practices; the Commission provided congressional testimony stating that the FTC deems inadequate data security to be a potentially unfair practice (*see* Prepared Statement of the Federal Trade Commission on Privacy in the Digital Age: Preventing Data Breaches and Combatting Cybercrime before the Senate Committee on the Judiciary (Feb. 4, 2014) at 3, *available at* https://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-digital-age-preventing-data-breaches-combating/140204 datasecuritycybercrime.pdf); Prepared Statement of the Federal Trade Commission before the Senate Committee on Science, Commerce, and Transportation (July 27, 2010) at 6, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy/100727consumerprivacy.pdf); and the Commission produced the 2007 Business Guide, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. The Commission also published information about the risks of inadvertent sharing through the use of P2P software, as well as issued a report and testified before Congress to provide information on the subject. (*See* CCFF ¶¶ 1338, 1340-1342,

1345, 1347, 1349-1351). All such guidance was available and applicable to HIPAA-covered entities.

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)).

Response to Finding No. 306:

The proposed finding is misleading to the extent that it suggests that outreach to all entities (e.g., information produced about data security), including HIPAA-covered entities such as LabMD, was not sufficient to inform those entities of what was expected of them to comply with Section 5. (*See* CCRRFF ¶ 305)).

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)).

Response to Finding No. 307:

The proposed finding is misleading to the extent that it suggests that the Commission had not provided sufficient information to inform all entities, including HIPAA-covered entities such as LabMD, of what was expected of them to comply with Section 5. (*See* CCRRFF ¶ 305).

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).

Response to Finding No. 308:

The Court should disregard the proposed finding because it is not supported by the citations to the record, as the pages to which LabMD cites (RX525 (Kaufman, Dep. at 190, 207-210)) do not exist and cannot support the proposed finding. Accordingly, the proposed finding is in violation of the Court's Order on Post-Trial Briefs.

The proposed finding also is incomplete and misleading to the extent that it suggests that there is not ample guidance available to companies to protect their information. (*See* Initial Pretrial Conference, *In re LabMD, Inc.*, FTC No. 9357, at 9-10) (Sept. 25, 2013) (MR. SHEER: "The Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness. In addition, there have been public statements made by the Commission, as well as educational materials that have been provided. And in addition, the industry, the IT industry itself, has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness"); CCRRFF ¶ 305).

Finally, the pre-hearing conference exchange to which Respondent cites is not evidence in this matter, and, regardless, this exchange contains a transcription error.

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)).

Response to Finding No. 309:

The Court should disregard proposed finding because it is irrelevant and not supported by the citation to the record. Discovery responses that Complaint Counsel provided to Respondent have no bearing on this proceeding since Respondent has not offered them into the record. In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

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)).

Response to Finding No. 310:

The Court should disregard the proposed finding because it is irrelevant and not supported by the citation to the record. Discovery responses that Complaint Counsel provided to Respondent, and that have not been admitted into the record, have no bearing on this proceeding.[10] In addition, Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding.

Further, because data security is a "continuous process of assessing and addressing risks," it should not be surprising that the Commission continues to produce materials to provide data security guidance to companies. (*See* Comm'n Statement Marking 50th Data Sec. Settlement

[10] Since Respondent's discovery requests were not time-limited (*see, e.g.*, RX518 (Compl. Counsel's Resps. to LabMD's First Set of Reqs. for Production and Interrogs.) at 9-10), Complaint Counsel fulfilled its discovery obligations by producing responsive documents in its initial responses to Respondent's discovery requests and in supplemental productions up until the close of the record.

(Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/

140131gmrstatement.pdf).

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)).

Response to Finding No. 311:

The proposed finding is irrelevant and not supported by the citation to the record.

(CCRRFF ¶ 310 (addressing substantively identical Proposed Finding 310)).

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)).

Response to Finding No. 312:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding. In addition, the proposed finding is misleading to the extent that the Commission has provided ample information and guidance with respect to data security that was available and applied to all entities, including LabMD. (*See* CCRRFF ¶ 305).

I. Dr. Hill

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)).

Response to Finding No. 313:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 314:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 315:

The proposed finding is incomplete and misleading. The materials Dr. Hill considered in forming opinions in her opening expert report, dated March 18, 2014, are identified in full elsewhere in the record. (*Compare* RX524 (Hill, Dep. at 59-60), *with* CX0740 (Hill Report) ¶¶ 46-47 (referencing Appendix B (CX0740 at 59-66)).

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)).

Response to Finding No. 316:

The proposed finding is misleading. Dr. Hill specifically testified as follows:

> Q. Would you agree that there is no one place where someone not of your education, background, experience, could go and find out what the industry and government standards and guidelines and vulnerability databases that establish best practices for information security practitioners?
> **A. No.**
> Q. There is one place you could go?
> **A. Yes.**
> Q. Where is that?
> **A. Google.**

(Hill, Tr. 91-92). Dr. Hill's testimony that Google is a resource for locating information on information security is not equivalent to her stating that Google is *the* only place where one learn of industry and government standards and guidelines. On the contrary, her reference to Google makes clear that it is easy for non-experts to find resources on information security using readily-accessible means.

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)).

Response to Finding No. 317:

The proposed finding is misleading and irrelevant. First, the proposed finding is ambiguous as to the meaning of "any other portions" of HIPAA—which could incorporate statutes, regulations, and guidance—and misleading. In addition to the security rule, Dr. Hill considered the article "6 Basics of Security Risk Analysis and Risk Management," published by HHS as part of its HIPAA Security Series (CX0405). (CX0740 (Hill Report) at 65; Hill, Tr. 232).

Second, LabMD is required to comply with the FTC Act irrespective of HIPAA. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't Mot. for Summ. Decision at 5-6 (May 19, 2014). Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")). Dr. Hill was not asked to provide an opinion on HIPAA. (RX524 (Hill, Dep. at 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)).

Response to Finding No. 318:

The proposed finding is compound, misleading, incomplete, and contradicted by the weight of the evidence.

Subsection (a) of the proposed finding is not supported by the citation to the record. Subsection (a) of the proposed finding is also incomplete and misleading. Dr. Hill testified that she considered the Security Rule promulgated under HIPAA. (Hill, Tr. 231, 246; CCFF ¶ 428). In addition, she also considered the article "6 Basics of Security Risk Analysis and Risk Management," published by HHS as part of its HIPAA Security Series (CX0405). (*See* CX0740 (Hill Report) at 65; Hill, Tr. 232)).

Subsection (b) of the proposed finding, as well as the statement "did not consult any medical industry data-security practices," is not supported by the citation to the record. Subsection (b) of the proposed finding is also incomplete and misleading. The industry standards on which Dr. Hill relied in forming her opinion are consistent with protection mechanisms and guidelines for protecting medical data. As Dr. Hill testified, in forming her opinions she relied on guidance from the National Research Council that provides guidelines for

protecting medical data. (CX0740 (Hill Report) at 66). Moreover, Dr. Hill explained that for purposes of protecting computer infrastructure, common guidelines are applied across all domains, including the protection of medical data. (Hill, Tr. 234-235 ("A: . . . Computing is pervasive, so these guidelines, whether they're from NIST or from the Computer Emergency Response Team or from the National Research Council that specifically focused on medical data, they have consistent guidelines. And that's because computing is pervasive and consistent across different types of business domains."); RX0524 (Hill, Dep. at 61-62 ("A: . . . these are standards that are used across . . . different types of industries as it relates to computer security")).

Subsection (c) of the proposed finding is incomplete and misleading. Dr. Hill properly considered data security measures applicable to LabMD. (Hill, Tr. 295-296) ("The recommendations that I laid out in my expert witness document contain basic requirements for securing a system. These are consistent with recommendations by governmental and industry and academic institutions working together to define and specify such recommendations. So it is expected that an organization will apply updates to their software. It is expected that they will have strong passwords. It would -- it is expected that they would implement access control mechanisms. It is expected that they would assess their networks for emerging vulnerabilities. So what I've recommended is what these other guidelines recommend. These are the basic things that you must do to have reasonable and appropriate security for your system. So I don't think the guidelines that I've put in place exceed what the other guidelines by those organizations are recommending. For both -- for small organizations and for large organizations, the guidelines are consistent.").

Furthermore, the layered strategy to provide reasonable data security that Dr. Hill describes, (CCFF ¶¶ 384-395), applies to companies of all sizes, and implicitly includes consideration of a company's size. For example, the amount of information and number of other resources that need to be protected may vary with the size of the company, such that a small company may have only a few servers and limited other resources to protect, while a larger company may have several hundred servers and thousands of resources to protect. (*See* CCFF ¶ 388). Thus, "specifying an appropriate set of security goals and policies for protecting those resources; and deploying mechanisms that are appropriately configured to enforce those policies" may also vary with the size of the company. (*See* CCFF ¶ 388). However, the volume and sensitivity of the information maintained within the network must also be considered, and LabMD maintained large amounts of highly sensitive Personal Information. (CCFF ¶¶ 392, 393; CX0740 (Hill Report) ¶ 32 (stating that "LabMD's network was small and simple"); CX0737 (Hill Rebuttal Report) ¶ 9 ("For LabMD, a reasonable data security strategy must take into account the large amounts of highly sensitive Personal Information, including Social Security numbers, medical insurance information, and medical diagnosis codes on its network.")).

Subsection (d) of the proposed finding is not supported by the citation to the record. Subsection (d) of the proposed finding is also incomplete and misleading. The principles for implementing a layered data security strategy to protect computer networks were widely available to LabMD from many sources during the relevant time period of January 2005 through July 2010. (CX0740 (Hill Report) at 64-65). For instance, the National Institute For Standards and Technology ("NIST"), published a standard that explained the risk management process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level in 2002. (CCFF ¶ 490; CX0400). Beginning in 2002, NIST Special Publication 800-30 (Risk

Management Guide for Information Technology Systems) explained a nine step process, beginning with cataloging network resources (including hardware, software, information, and connections) to define the scope of risk assessment, moving through vulnerability identification and cost-benefit analyses of measures that could mitigate the risk of a vulnerability, and ending with security measure recommendations and a written record of the process. (CCFF ¶ 491). These primary steps included methods and tools that could be used to perform them. (CCFF ¶ 492). Similarly, in 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central principles of NIST SP 800-30 in explaining how to perform the risk analysis required by the HIPAA Security Rule and sets out examples of common steps for risk analysis and risk management. (CCFF ¶ 493; CX0405 (HIPAA Security Series 6 - Basics of Risk Analysis and Risk Management)).

Subsection (e) of the proposed finding is not supported by the citation to the record. Subsection (e) of the proposed finding is also incomplete and misleading. The industry standards on which Dr. Hill relied in forming her opinion are consistent with protection mechanisms and guidelines for protecting medical data. As Dr. Hill testified, in forming her opinions she relied on guidance from the National Research Council that provides guidelines for protecting medical data. (CX0740 (Hill Report) at 66). Moreover, Dr. Hill explained that for purposes of protecting computer infrastructure, common guidelines are applied across all domains, including the protection of medical data. (Hill, Tr. 234-235 ("A: . . . Computing is pervasive, so these guidelines, whether they're from NIST or from the Computer Emergency Response Team or from the National Research Council that specifically focused on medical data, they have consistent guidelines. And that's because computing is pervasive and consistent

across different types of business domains."; RX0524 (Hill, Dep. at 61-62 ("A: . . . these are standards that are used across . . . different types of industries as it relates to computer security")).

Complaint Counsel has no specific response to subsection (f).

The portion of the proposed finding which states, "did not apply the Commission's 'reasonable' test but rather a more stringent 'best practices' test," is not supported by the citation to the record. This portion of the proposed finding is also incomplete and misleading. Dr. Hill properly concluded that LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network, and that LabMD could have corrected its security failures at relatively low cost using readily available security measures. (CX0740 (Hill Report) ¶ 4).

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).

Response to Finding No. 319:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 320:

The proposed finding is misleading. Dr. Hill's report lists all the information in addition to the HIPAA security rule that she considered in reaching her opinion. (RX524 (Hill, Dep. at 61)). Dr. Hill also testified that she was not asked to provide an opinion on HIPAA. (RX524 (Hill, Dep. at 66)).

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).

Response to Finding No. 321:

The proposed finding is misleading to the extent that it implies that the HHS article concerning six basic principles of risk assessment is a part of the HIPAA statute or regulation. As indicated in the appendix to her report, the cited portion of Dr. Hill's testimony referred to the article "HIPAA Security Series 6: Basics of Security Risk Analysis and Risk Management," published by HHS as part of its HIPAA Security Series. (*See* CX0740 (Hill Report) at 65; Hill, Tr. 232). This is an informational publication "to provide assistance to entities required to comply with HIPAA security standards. (CX0405 (HIPAA Security Series 6: Basics of Risk Analysis and Risk Management) at 1).

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

Response to Finding No. 322:

The proposed finding is misleading. Dr. Hill testified only that she could not "make a statement or – about the legal aspects of HIPAA and what it governs." (Hill, Tr. 231).

The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't Mot. for Summ. Decision at 5-6 (May 19, 2014). Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

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.").

Response to Finding No. 323:

The proposed finding is irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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

Response to Finding No. 324:

The proposed finding is irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 325:

The proposed finding is irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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

Response to Finding No. 326:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Dr. Hill testified that, in her opinion, LabMD's *policy* on physical security

in its Employee Handbook was acceptable, not that its actual physical data security as practiced was adequate. (RX524 (Hill, Dep. at 118-19)).

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)).

Response to Finding No. 327:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 328:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 329:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Dr. Hill's report does not assume likelihood of harm. The cited portion of the report states only that she assumed that the types of information in LabMD's possession "can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information. (CX0740 (Hill Report) ¶ 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)).

Response to Finding No. 330:

The proposed finding is misleading and irrelevant. While CX0019 was among the documents included in Appendix B of Dr. Hill's report, Respondent does not cite to a portion of

her report that depended on or involved that document. Furthermore, Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony.

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)).

Response to Finding No. 331:

The proposed finding is irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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

Response to Finding No. 332:

The Court should disregard the proposed finding because it is irrelevant and attempts to state a legal conclusion. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 333:

The proposed finding is misleading. To the extent the proposed finding asserts that Dr. Hill did not rely on data security business guidance published by the FTC, FTC guidance is consistent with Dr. Hill's approach and other data security standards and guidance that Dr. Hill considered, and that are available to companies, and Dr. Hill relied on the only relevant test for whether data security practices are unfair under Section 5: reasonableness. (CCRRFF ¶ 88 (addressing substantively identical Proposed Finding 88); *see also* CCRRFF ¶ 340 (describing how FTC-published guidance is consistent with Dr. Hill's opinion); CCRRCL ¶ 145).

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)).

Response to Finding No. 334:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. Furthermore, the proposed finding is irrelevant and misleading. Dr. Hill properly considered data security measures applicable to LabMD. (Hill, Tr. 295-96 ("The recommendations that I laid out in my expert witness document contain basic requirements for securing a system. These are consistent with recommendations by governmental and industry and academic institutions working together to define and specify such recommendations. So it is expected that an organization will apply updates to their software. It is expected that they will have strong passwords. It would -- it is expected that they would implement access control mechanisms. It is expected that they would assess their networks for emerging vulnerabilities. So what I've recommended is what these other guidelines recommend. These are the basic things that you must do to have reasonable and appropriate security for your system. So I don't think the guidelines that I've put in place exceed what the other guidelines by those organizations are recommending. For both -- for small organizations and for large organizations, the guidelines are consistent.")). *See also* CCRRFF ¶ 318 (layered strategy to provide reasonable

data security applies to companies of all sizes and implicitly includes consideration of company's size, but volume and sensitivity of information must also be taken into account).

The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

332a. "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)).

Response to Finding No. 332a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

333a. "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)).

Response to Finding No. 333a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply

with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

333b. 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)).

Response to Finding No. 333b:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

334a. 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).

Response to Finding No. 334a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 335:

The proposed finding is misleading. Dr. Hill has over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems. (CCFF ¶¶ 16-18).

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)).

Response to Finding No. 336:

The proposed finding is misleading. Dr. Hill has over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems. (CCFF ¶¶ 16-18).

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)).

Response to Finding No. 337:

The proposed finding is misleading. Dr. Hill has over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems. (CCFF ¶¶ 16-18).

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)).

Response to Finding No. 338:

The proposed finding is misleading. While Dr. Hill did testify that she based the definition of "comprehensive information security program" found in her report on her extensive experience in the field, she also testified that her conclusions aligned with "government standards and guidelines." (RX524 (Hill, Dep. at 85-86)).

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)).

Response to Finding No. 339:

The proposed finding is misleading. While Dr. Hill did testify that she based the conclusions set forth in her report primarily on her extensive background and experience in the field, she also testified that her conclusions aligned with "government standards and guidelines." (RX524 (Hill, Dep. at 85-86)).

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)).

Response to Finding No. 340:

The proposed finding is compound, misleading, incomplete, and contradicted by the weight of the evidence. The principles for implementing a layered data security strategy to protect computer networks were widely available to LabMD from many sources during the relevant time period of January 2005 through July 2010. (CCFF ¶¶ 489-498; CX0740 (Hill Report) at 64-65). The five basic steps described in the Commission's 24-page "*Protecting Personal Information*" business guide are: (1) Take Stock: Know what personal information you have in your files and on your computers. (2) Scale Down: Keep only what you need for your business. (3) Lock it: Protect the information that you keep (covering both physical and electronic security) (4) Pitch it: Properly dispose of what you no longer need. (5) Plan Ahead: Create a plan to respond to security incidents. FTC, *Protecting Personal Information: A Guide for Business* at 3, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. These considerations are consistent with the network security principles identified by Dr. Hill. Indeed, implementing reasonable security requires consideration of, and of course reliable implementation of, fundamental data security principles, no matter how they are articulated.

Both Dr. Hill's report and *Protecting Personal Information* address these fundamental data security principles. Dr. Hill's "Don't Keep What You Don't Need" (CX0740 (Hill Report) ¶ 31(a)), is the same concept as "Scale down. Keep only what you need for your business." *Protecting Personal Information* at 2, 6-9. Dr. Hill's "Patch" admonition (CX0740 ¶ 31(b)), is the same as the guide's recommendation to "check expert websites (such as www.sans.org) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems." *Protecting Personal*

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

Similarly, the National Institute For Standards and Technology ("NIST"), published a standard that explained the risk management process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level in 2002. (CCFF ¶ 490; CX0400 (NIST Special Publication 800-30 dated July 2002)). Beginning in 2002, NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) explained a nine step process, beginning with cataloging network resources (including hardware, software, information, and

connections) to define the scope of risk assessment, moving through vulnerability identification and cost-benefit analyses of measures that could mitigate the risk of a vulnerability, and ending with security measure recommendations and a written record of the process. (CCFF ¶ 491). These primary steps included methods and tools that could be used to perform them. (CCFF ¶ 492). Similarly, in 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central principles of NIST SP 800-30 in explaining how to perform the risk analysis required by the HIPAA Security Rule and sets out examples of common steps for risk analysis and risk management. (CCFF ¶ 493; CX0405 (HIPAA Security Series 6: Basics of Risk Analysis and Risk Management) at 3, 5-16).

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)).

Response to Finding No. 341:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also misleading to the extent it mischaracterizes LabMD's Request for Admission No. 1, which states as follows:

> Admit that between 2005 and the present the FTC has not prescribed any rules or promulgated regulations regarding data-security, data security practices or data security standards for Protected Health Information ("PHI") pursuant to its authority under 15 U.S.C. § 57a(a).

(RX526 (Compl. Counsel's Amended Resp. to LabMD, Inc.'s 1st Set of Reqs. for Admission) at 4, Resp. to Req. 1). The request for admission addresses only "rules" or "regulations" promulgated under 15 U.S.C. § 57a(a), and does not extend to "standards or guidance." The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective

of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant.

(CCRRFF ¶ 322).

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)).

Response to Finding No. 342:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 343:

The Court should disregard the proposed finding because it is not supported by the citations to the record, as the pages to which LabMD cites (RX525 (Kaufman, Dep. at 211, 215)) do not exist and cannot support the proposed finding. Accordingly, the proposed finding is in violation of the Court's Order on Post-Trial Briefs.

The proposed finding is also not supported by the quoted testimony. The quoted testimony shows only that Mr. Kaufman testified that the term "data security" does not appear in Section 5 and that the FTC has not promulgated regulations regarding data security. Mr. Kaufman specifically testified that the "Bureau and the Commission have consistently applied the reasonableness test to Section 5 data security cases. (RX532 (Kaufman, Dep. at 211)).

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.").

Response to Finding No. 344:

The proposed finding is incorrect. Dr. Hill testified that she did not assume that the 1718 file was exposed due to inadequate security, but reached this conclusion based on her review of the evidence. (Hill, Tr. 219-20).

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).

Response to Finding No. 345:

The proposed finding is misleading. The manner in which the 1718 file was exposed is not a matter of expert opinion, but of fact. The record is clear that the 1718 file was shared on the Gnutella network as a result of the LimeWire client installed on a LabMD computer. (CCFF ¶¶ 1363-1372 (§ 7.1.2 1718 File Shared on Gnutella Network Through LimeWire on a LabMD Billing Computer)). Dr. Hill concluded that the LimeWire software was on the LabMD computer as a result of LabMD's unreasonable data security. (CX0740 (Hill Report) ¶ 105).

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)).

Response to Finding No. 346:

Complaint Counsel has no specific response.

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

Response to Finding No. 347:

The proposed finding is misleading. The manner in which the 1718 file was exposed is not a matter of expert opinion, but of fact. (CCRRFF ¶ 345)).

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)).

Response to Finding No. 348:

The proposed finding is irrelevant and misleading. Dr. Hill properly considered data security measures applicable to LabMD, including practices in light of the size and complexity of its business and the Personal Information it collected and maintains. (CCRRFF ¶¶ 318, 334).

The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 349:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 350:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 351:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 352:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 353:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 354:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 355:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 356:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

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)).

Response to Finding No. 357:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

355a. 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)).

Response to Finding No. 355a:

The proposed finding is irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322). In addition, the proposed finding is incorrect. Dr. Hill testified that she considered the Security Rule promulgated under HIPAA. (Hill, Tr. 231, 246). In addition, Dr. Hill testified that she considered the document HIPAA Security Series 6 - Basics of Risk Analysis and Risk Management, promulgated by HHS (CX0405). (Hill, Tr. 232; CX0740 (Hill Report) at 65).

356a. 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)).

Response to Finding No. 356a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. The proposed finding is also misleading. Dr. Hill properly considered data security measures applicable to LabMD. (CCRRFF ¶ 334).

The proposed finding is also irrelevant. LabMD is required to comply with the FTC Act irrespective of HIPAA and Respondent has conceded that its Compliance with HIPAA is irrelevant. (CCRRFF ¶ 322).

357a. 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)).

Response to Finding No. 357a:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 358:

The proposed finding is misleading and contradicted by the weight of the evidence. Dr. Hill has offered opinions that specify precisely how LabMD failed to provide reasonable and appropriate security for Personal Information within its computer network throughout the relevant time period of January 2005 through July 2010, and opined on how LabMD could have corrected its security failures at relatively low cost using readily available security measures. (*See* Hill, Tr. 95-96, 124, 203; CX0740 (Hill Report) ¶¶ 49, 107; CX0737 (Hill Rebuttal Report) ¶¶ 5, 31; CCFF ¶¶ 1113-1185 (§ 5 LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures). Tellingly, LabMD does not cite with specificity

any evidence or admissions in the record to support its proposed finding, in violation of the Court's Order on Post-Trial Briefs.

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)).

Response to Finding No. 359:

Complaint Counsel has no specific response.

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).

Response to Finding No. 360:

The proposed finding mischaracterizes Dr. Hill's opinions. Based on a thorough review of the facts of this case and her experience and professional qualifications, Dr. Hill opined that companies should consider certain key principles when implementing a layered defense strategy to protect their computer networks. (CCFF ¶ 394). Those key principles include: (1) Don't keep what you don't need; (2) Patch software; (3) Close unused ports; (4) Create and implement security policies; (5) Protect the network with security software; (6) Probe the network with periodic audits, including penetration testing; and (7) Create and implement policies that govern the physical access to devices and data. (CCFF ¶ 394).

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)).

Response to Finding No. 361:

The proposed finding is misleading. Based on a thorough review of the facts of this case and her experience and professional qualifications, Dr. Hill opined that companies should consider certain key principles when implementing a layered defense strategy to protect their computer networks. (CCFF ¶ 394). Those key principles include: (1) Don't keep what you

don't need; (2) Patch software; (3) Close unused ports; (4) Create and implement security policies; (5) Protect the network with security software; (6) Probe the network with periodic audits, including penetration testing; and (7) Create and implement policies that govern the physical access to devices and data. (CCFF ¶ 394).

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

Response to Finding No. 362:

The proposed finding mischaracterizes Dr. Hill's testimony and is irrelevant. Dr. Hill has provided uncontroverted testimony that she relied on widely known and accepted guidance from multiple sources to formulate her opinions regarding key principles companies should consider when implementing a layered defense strategy. (Hill, Tr. 242-245; CCFF ¶ 394; CX0740 (Hill Report) at 64-65). Indeed, Dr. Hill's report lists in Appendix B materials considered or relied upon, including over fourteen articles and publications issued by entities including the U.S. Department of Health and Human Services, NIST, the SANS Institute, and the Internet Security Alliance. (CX0740 (Hill Report) at 64-65). Moreover, as Dr. Hill explained, concepts such as patching software, closing unused ports, and specifying strong password policies "are captured in general guidelines" and "are very basic recommendations that anyone would use to protect their infrastructure." (Hill, Tr. 245).

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)).

Response to Finding No. 363:

The proposed finding mischaracterizes Dr. Hill's opinions. The industry standards on which Dr. Hill relied in forming her opinion are consistent with protection mechanisms and guidelines for protecting data such as names, dates of birth, SSNs, CPT codes for tests to be

performed, and health insurance provider names, addresses, and policy numbers. (*Cf.* CCFF ¶ 125 (types of information in insurance aging reports)). As Dr. Hill testified, in forming her opinions she also relied on guidance from the National Research Council that provides guidelines for protecting medical data. (CX0740 (Hill Report) at 66). Moreover, Dr. Hill explained that for purposes of protecting computer infrastructure, common guidelines are applied across all domains, including the protection of medical data. (Hill, Tr. 234-235 ("A: . . . Computing is pervasive, so these guidelines, whether they're from NIST or from the Computer Emergency Response Team or from the National Research Council that specifically focused on medical data, they have consistent guidelines. And that's because computing is pervasive and consistent across different types of business domains."; RX0524 (Hill, Dep. at 61-62 ("A: . . . these are standards that are used across . . . different types of industries as it relates to computer security.")).

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

Response to Finding No. 364:

The proposed finding is irrelevant. The industry standards on which Dr. Hill relied in forming her opinion are consistent with protection mechanisms and guidelines for protecting medical data. (CCRRFF ¶ 363).

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

Response to Finding No. 365:

The proposed finding mischaracterizes Dr. Hill's testimony and is irrelevant. It is well-settled that the principles for implementing a layered data security strategy to protect computer networks were widely available to LabMD from many sources during the relevant time period of

January 2005 through July 2010. (CX0740 (Hill Report) at 64-65). For instance, the National Institute For Standards and Technology ("NIST"), published a standard that explained the risk management process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level in 2002. (CCFF ¶ 490; CX0400). Beginning in 2002, NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) explained a nine step process, beginning with cataloging network resources (including hardware, software, information, and connections) to define the scope of risk assessment, moving through vulnerability identification and cost-benefit analyses of measures that could mitigate the risk of a vulnerability, and ending with security measure recommendations and a written record of the process. (CCFF ¶ 491). These primary steps included methods and tools that could be used to perform them. (CCFF ¶ 492). Similarly, in 2005, the Centers for Medicare and Medicaid Services published HIPAA Security Series 6: Basics of Risk Analysis and Risk Management, which incorporates the central principles of NIST SP 800-30 in explaining how to perform the risk analysis required by the HIPAA Security Rule and sets out examples of common steps for risk analysis and risk management. (CCFF ¶ 493; CX0405).[11] Based on general industry guidance and guidance specific to the medical industry available during the relevant time period, LabMD knew or should have known to implement a layered defense strategy to protect its computer networks.

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)).

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

Response to Finding No. 366:

The proposed finding is misleading, irrelevant, and contradicted by the weight of the evidence. Complaint Counsel agrees that Mr. Kaloustian testified that penetration testing was never done. (CX0735 (Kaloustian, IHT at 92, 281-282)). The proposed finding, however, is misleading and contradicted by the weight of the evidence insofar as the proposed finding suggests that Mr. Kaloustian is the only witness to testify that penetration testing was never done.

The proposed finding is contradicted by the evidentiary record as multiple witnesses testified that LabMD did not use penetration testing before 2010. (CCFF ¶¶ 715-726 (§ 4.3.4 LabMD Did Not Use Penetration Testing Before 2010); CX0734 (Simmons, IHT at 67-68) ("I don't recall us ever doing anything like that [a penetration test].")).

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).

Response to Finding No. 367:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 368:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Dr. Hill's report states that personal information was transmitted and stored in an *unencrypted* format. (CX0740 (Hill Report) ¶ 91(f) (emphasis added). To the extent the proposed finding argues that Dr. Hill's statement that personal information was transmitted and stored in an unencrypted format relies only on Mr. Kaloustian, the proposed finding is

misleading and contradicted by the weight of the evidence. Dr. Hill cites to Mr. Kaloustian's testimony as an example. (CX0740 (Hill Report) ¶ 91(f) n.37). Complaint Counsel agrees that Mr. Kaloustian testified that personal information was transmitted and stored in an unencrypted format. (CX0735 (Kaloustian, IHT at 62-64, 302-304)). But Alison Simmons also testified that personal information was stored in an unencrypted format. (CX0734 (Simmons, IHT at 43)).

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)).

Response to Finding No. 369:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 370:

The proposed finding is misleading, irrelevant, and contradicted by the weight of the evidence. Complaint Counsel agrees that Mr. Kaloustian testified 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. (CX0735 (Kaloustian, IHT at 98-104)). The proposed finding, however, is misleading and contradicted by the weight of the evidence insofar as the proposed finding suggests that Mr. Kaloustian is the only witness to testify that firewalls were not configured to prevent unauthorized traffic from entering the network.

The proposed finding is contradicted by the evidentiary record as multiple witnesses testified that firewalls were not configured to prevent unauthorized traffic from entering the network. (CX0730 (Simmons, IHT at 53-54) ("there were other computers that weren't locked

down by that firewall"); CX0734 (Simmons, IHT at 101-102) (LabMD did not limit the web sites that Michael Daugherty, John Boyle, IT staff, the lab manager, the billing manager, and the pathologist could visit online); CCFF ¶¶ 1094-1105 (§ 4.8.3.2 LabMD Did Not Properly Configure Its Firewall to Block IP Addresses and Unnecessary Ports); CX0067 (Providyn Network Security Scan – LabNet) at 22 (the ProviDyn external vulnerability scans show that not only was port 10,000 open in 2010, but also that LabMD's Veritas backup application had not been updated to correct the vulnerability that Symantec identified)).

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

Response to Finding No. 371:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 372:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 373:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Kaloustian's testimony does not reference or otherwise support that there was a notification to Commission staff by LabMD's counsel.

Moreover, to the extent the proposed finding asserts that it was improper for Commission staff to contact a former employee without first informing the company's legal counsel, the

Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. As a legal conclusion, the assertion is not supported by any citation and is a misstatement of law. Complaint Counsel had no obligation to inform LabMD prior to conducting an investigational hearing of one of its former employees, who no longer has a business relationship with the company. Commission Rules do not require Complaint Counsel to seek consent from a company prior to conducting an investigational hearing of one of its former employees. While it is customary to contact counsel prior to dealing with employees of a represented party, FTC Operating Manual § 3.3.6.3, *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch03investigations_0.pdf, Mr. Kaloustian is not an employee of LabMD. He is a former employee, with no continuing relationship with LabMD. (CX0735 (Kaloustian, IHT at 9). The FTC Operating Manual does not require Complaint Counsel to notify opposing counsel when it interviews former employees or third party witnesses. FTC Operating Manual § 3.6.7.6.3.2, *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch03investigations_0.pdf.

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

Response to Finding No. 374:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Kaloustian's testimony does not reference or otherwise support the proposed finding that LabMD was not informed of Mr. Kaloustian's investigational hearing.

To the extent Respondent is attempting to assert that Complaint Counsel had an obligation to inform LabMD prior to conducting an investigational hearing of one of its former employees, who no longer has a business relationship with the company, this assertion is legally unavailing. Commission Rules do not require Complaint Counsel to seek consent from a

company prior to conducting an investigational hearing of one of its former employees, such as Mr. Kaloustian. (CCRRFF ¶ 373). Witnesses have the right to proceed with or without counsel. Commission Rule of Practice 2.9(b), 16 C.F.R. § 2.9(b). Mr. Kaloustian was informed it was his choice to proceed with his own counsel, counsel to LabMD, or without counsel, and he proceeded without counsel. (CX0735 (Kaloustian, IHT at 10)).

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)).

Response to Finding No. 375:

The Court should disregard the proposed finding because it is not supported by the citation to the record, and attempts to state a legal conclusion. To the extent Respondent is attempting to assert that it has a right to participate in the investigational hearings of its former employees, who no longer have a business relationship with the company, this assertion is legally unavailing. Commission Rules do not require Complaint Counsel to seek consent from a company prior to conducting an investigational hearing of one of its former employees, such as Mr. Kaloustian. (CCRRFF ¶ 373). Witnesses have the right to proceed with or without counsel. Commission Rule of Practice 2.9(b), 16 C.F.R. § 2.9(b). Mr. Kaloustian was informed it was his choice to proceed with his own counsel, counsel to LabMD, or without counsel, and he proceeded without counsel. (CX0735 (Kaloustian, IHT at 10)).

376. At the time he testified to FTC on May 3, 2013, [redacted] **}**[12]. (RX 415 (Kaloustian background check/A. Simmons' resignation, at 1)) ("Terminated for failure to perform job duties").

[12] RX415 was granted permanent *in camera* treatment on the basis of sensitive personal information. Order Granting Jt. Mot. for *In Camera* Treatment of Ex. Containing Sensitive Personal Information (May 15, 2014). Respondent's proposed finding does not disclose the sensitive personal information contained therein. Nonetheless, Complaint Counsel has identified as *in camera* information quoted or derived from RX415 to comply with the Order.

Response to Finding No. 376:

To the extent the proposed finding is a quotation of RX415 [redacted], Complaint Counsel has no specific response. To the extent the proposed finding asserts that [redacted], however, it is contradicted by Mr. Kaloustian's testimony. (CX0735 (Kaloustian, IHT at 304-07) (testifying that he was terminated for "job abandonment" for refusing to cut short a preapproved vacation and return to work at Mr. Boyle's demand)).

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)).

Response to Finding No. 377:

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

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).

Response to Finding No. 378:

The proposed finding is misleading. To the extent the proposed finding asserts that Dr. Hill did not rely on data security business guidance published by the FTC, FTC guidance is consistent with Dr. Hill's approach and other data security standards and guidance that Dr. Hill considered, and that are available to companies, and Dr. Hill relied on the only relevant test for whether data security practices are unfair under Section 5: reasonableness. (CCRRFF ¶ 88 (addressing substantively identical Proposed Finding 88); *see also* CCRRFF ¶ 340 (describing how FTC-published guidance is consistent with Dr. Hill's opinion); CCRRCL ¶ 145).

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)).

Response to Finding No. 379:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 380:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 381:

To the extent it asserts that Dr. Hill relied on evidence from Boback and Tiversa for her opinion regarding likelihood of harm, the proposed finding is misleading. Dr. Hill relied on the testimony of Mr. Boback only for the proposition that the copies of the 1718 File "were found on computers in California, Arizona, Costa Rica, and the United Kingdom." (CX0740 (Hill Report) ¶ 43, 43 n.6). Regardless, the proposed finding is irrelevant, because Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. To the extent the proposed finding asserts that evidence related to Tiversa is perjured and fraudulent, it is unsupported by the citations to the record.

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)).

Response to Finding No. 382:

The proposed finding is misleading and incomplete. Dr. Hill has provided uncontroverted testimony that she relied on widely known and accepted guidance from multiple sources to formulate her opinions regarding key principles companies should consider when implementing a layered defense strategy. (Hill, Tr. 242-245; CCFF ¶ 394; CX0740 (Hill Report) at 64-65). Indeed, Dr. Hill's report lists in Appendix B materials considered or relied upon, including over fourteen articles and publications issued by entities including the U.S. Department of Health and Human Services, NIST, the SANS Institute, and the Internet Security Alliance. (CX0740 (Hill Report) at 64-65). Moreover, as Dr. Hill explained, concepts such as patching software, closing unused ports, and specifying strong password policies "are captured in general guidelines" and "are very basic recommendations that anyone would use to protect their infrastructure." (Hill, Tr. 245).

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

Response to Finding No. 383:

The proposed finding is misleading. To the extent the proposed finding asserts that Dr. Hill did not rely on data security business guidance published by the FTC, FTC guidance is consistent with Dr. Hill's approach and other data security standards and guidance that Dr. Hill considered, and that are available to companies, and Dr. Hill relied on the only relevant test for whether data security practices are unfair under Section 5: reasonableness. (CCRRFF ¶ 88 (addressing substantively identical Proposed Finding 88); *see also* CCRRFF ¶ 340 (describing how FTC-published guidance is consistent with Dr. Hill's opinion); CCRRCL ¶ 145).

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)).

Response to Finding No. 384:

The Court should disregard the proposed finding because it is not supported by specific citations to the record, in violation of the Court's Order on Post-Trial Briefs. Rather than cite specific pages or portions of evidence to support its position, LabMD has improperly cited to the entirety of Dr. Hill's deposition testimony, Dr. Hill's opening expert report, and Dr. Hill's hearing testimony.

In addition, the proposed finding is contradicted by the record. Complaint Counsel asked Dr. Hill "to assess whether LabMD provided reasonable and appropriate security for Personal Information with in its computer network." (CX0740 (Hill Report) ¶ 45). Dr. Hill defined the Relevant Time Period for her opinion because "there [were] not sufficiently diverse types of information available after the Relevant Time Period for [her] to offer opinions about that period." (*Id.* ¶ 48).

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)).

Response to Finding No. 385:

The proposed finding is unsupported by specific references to the record, in violation of the Court's Order on Post-Trial Briefs. Rather than cite specific pages or portions of evidence to support its position, LabMD has improperly cited to the entirety of Dr. Hill's deposition testimony, Dr. Hill's opening expert report, and Dr. Hill's hearing testimony.

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)).

Response to Finding No. 386:

Complaint Counsel has no specific response.

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]; (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)).

Response to Finding No. 387:

To the extent that it assert that Mr. Kam was paid $350 per hour for her services as an expert in this case, Complaint Counsel has no specific response. To the extent the proposed finding asserts as facts the arguments it quotes from Respondent's denied Motions *in Limine*, the Court should disregard the proposed finding because it is not supported by any citation to the record, in violation of the Court's Order on Post-Trial Briefs, and is contradicted by the weight of the evidence. (*See* CCRRCL ¶ ¶ 179-189).

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

Response to Finding No. 388:

The proposed finding of fact is misleading to the extent it suggests that Mr. Kam's only education is his academic degree. Mr. Kam is also a Certified Information Privacy Professional (CIPP/US). Mr. Kam leads and participates in several cross-industry data privacy groups, regularly publishes relevant articles in the field, and works on development of policy and

solutions to address the protection of health information and personally identifiable information, as well as remediating privacy incidents, identity theft, and medical identity theft. (CX0742 (Kam Report) at 3-5, 25, 29-33).

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

Response to Finding No. 389:

The proposed finding is irrelevant. Mr. Kam was not offered as an expert on computer network security. (CX0742 (Kam Report) at 5 (offering an opinion as to the risk of injury to consumers resulting from the unauthorized disclosure of their sensitive personal information)).

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)).

Response to Finding No. 390:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The citation to the Mr. Kam's report only sets forth the contours of Mr. Kam's approach to his opinion. The portion of Mr. Kam's deposition cited does not state that his approach is not accepted in these fields nor does it state that no work based upon similar methodology has been published or peer reviewed.

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.").

Response to Finding No. 391:

The proposed finding is irrelevant. Mr. Kam's methodology is not based on statistical analysis, but is instead based on his extensive experience assisting companies remediate consumer harm resulting from remediating privacy incidents, identity theft, and medical identity theft. (Kam, Tr. 406-07; CX0742 (Kam Report) at 3-6).

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

Response to Finding No. 392:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The testimony cited by Respondent does not establish that Mr. Kam's methodology used in this case has never been "reviewed in any form." (Kam, Tr. 552 (discussing only whether Mr. Kam has published his methodology in a peer-reviewed format)).

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)).

Response to Finding No. 393:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Respondent's citation to its own Motion to establish a fact is in violation of the Court's Order on Post-Trial Briefs.

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] .

Response to Finding No. 394:

The proposed finding is misleading. Mr. Kam's methodology was described fully in his report, which Respondent received prior to the evidentiary hearing and could have been reviewed by an expert of Respondent's choosing. (CX0742 (Kam Report)).

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)).

Response to Finding No. 395:

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

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

Response to Finding No. 396:

Complaint Counsel has no specific response.

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).

Response to Finding No. 397:

The proposed finding is irrelevant.

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

Response to Finding No. 398:

The Court should disregard the proposed finding because it is not supported by the citation to the record and is irrelevant. Respondent has cited no evidence on the record that Dr. Ponemon served on Tiversa's board of advisors. Mr. Kam's testimony that he had heard this fact

is inadmissible hearsay. (*See* Kam, Tr. 552-553). Mr. Kam's knowledge of this unsupported claim is irrelevant.

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

Response to Finding No. 399:

Complaint Counsel has no specific response.

400. [redacted]**.).**

Response to Finding No. 400:

The Court should disregard the proposed finding because it is not supported by the citation to the record and is irrelevant. The citation does not support the claim that Mr. Kam paid $12,500 for the 2013 Ponemon Survey.

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

Response to Finding No. 401:

The proposed finding is irrelevant.

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

Response to Finding No. 402:

Complaint Counsel has no specific response.

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

Response to Finding No. 403:

The Court should disregard the proposed finding because it is irrelevant. Respondent has cited to no evidence explaining the significance or relevance of the Ponemon Study's response rate.

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.").

Response to Finding No. 404:

The proposed finding is irrelevant. Respondent has not cited to any relevant evidence or authority on the definition of regression analysis, whether it would be appropriate in this case, or whether such an analysis would have produced relevant information in this case.

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.").

Response to Finding No. 405:

The Court should disregard the proposed finding because it is irrelevant. Respondent has cited to no evidence to establish the definition or significance of non-response bias.

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.").

Response to Finding No. 406:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, and is not supported by the citation to the record. Respondent has cited to no

evidence that would support the finding that web-based surveys or survey with compensated respondent are unreliable.

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. . . .").

Response to Finding No. 407:

The proposed finding is irrelevant. Respondent has cited to no evidence to establish the definition or significance of sampling frame bias. In addition, Respondent has not pointed to any nonresponse or sampling biases that affected the reliability or outcome of the survey.

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).

Response to Finding No. 408:

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

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).

Response to Finding No. 409:

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

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.").

Response to Finding No. 410:

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

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.").

Response to Finding No. 411:

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

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

Response to Finding No. 412:

The proposed finding is irrelevant. Complaint Counsel's post-trial brief and proposed findings of fact do not cite to CX0451 (*in camera*) except for purposes of reserving its right to appeal exclusion of CX0451. (*See* CCFF ¶¶ 52 n.1, 1724, 1724 n.2).

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)).

Response to Finding No. 413:

The proposed finding is irrelevant. (*See* CCRRFF ¶ 412).

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

Response to Finding No. 414:

The proposed finding is misleading and irrelevant. Mr. Kam testified that he "didn't confirm any specific victims of identity theft from the LabMD disclosure because it was not best practice for me to reach out to those individuals, as I mentioned earlier, based on those circumstances." (Kam, Tr. 507). To the extent that the proposed finding asserts that LabMD's inadequate security practices did not injure consumers, the proposed finding is irrelevant. The consumer injury component of Section 5's unfairness test is satisfied when security practices are likely to cause injury. (CCCL ¶¶ 12, 24-27). The proposed finding is also misleading to the extent it implies that victims of LabMD's disclosures and practices would necessarily be identifiable. (*See, e.g.*, CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer to know which company was the source of the information that was then used to harm them, when a consumer does experience a harm.")).

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.").

Response to Finding No. 415:

The proposed finding is misleading and irrelevant, to the extent that it asserts that LabMD's inadequate security practices did not injure consumers. (CCRRFF ¶ 414 (addressing substantively identical Proposed Finding 414).

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.").

Response to Finding No. 416:

The proposed finding is irrelevant. Mr. Kam was not offered as an expert on computer network security.

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.").

Response to Finding No. 417:

The proposed finding mischaracterizes Mr. Kam's testimony. Mr. Kam did not testify regarding "all times relevant to this case." (*See* Kam, Tr. 517-518).

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)).

Response to Finding No. 418:

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

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)).

Response to Finding No. 419:

The Court should disregard the proposed finding because it is not supported by the citation the record. Mr. Kam's testimony makes it clear that he did not *assume* that the suspects were convicted of identity theft charges prior to the events in Sacramento on October 5, 2012. Rather, he based his opinion on Detective Jestes' testimony. (RX522 (Kam, Dep. at 147-48)).

Furthermore, the proposed finding is misleading and incomplete to the extent it suggests Mr. Kam's opinion is based on the fact that the individuals in whose possession LabMD Day Sheets and copied checks were found in Sacramento, California, were convicted *prior* to that point of identity theft, rather than arising out of that incident. He testified:

> Q. So how were they known identity thieves with respect to the LabMD matter in your mind, in your testimony, and your expert report?
> A. Okay. Detective Jestes said in her testimony that these two individuals were found with various item used to commit identity theft, including washed checks, software to create checks, other – utility bills with other people's names on them. My opinion is that these individuals were committing identity theft based on what I read in Detective Jestes' testimony and, therefore, has a risk factor, I ascribe a risk of possible identity theft to this particular situation in my analysis.

(RX522 (Kam, Dep. at 148)). Mr. Kam based his opinion on the fact that LabMD Day Sheets and copied checks were found in the possession of persons who pled no contest to identity theft charges. (*See* CX0742 (Kam Report) at 22; Kam, Tr. 455-56). It is irrelevant to his opinion whether they were convicted *before* they were found possessing LabMD Day Sheets and copied

checks, or *soon afterward*—which is the case (CX0720 (Jestes, Dep. at 43-44) (suspects arrested in conjunction with documents found at house in Sacramento, California, including LabMD Day Sheets and copied checks, were prosecuted for the crime of identity theft, for which they were arrested, and pled *nolo contendere*). In either case, the acts of identity theft for which they were convicted happened before their arrest, at the same time they possessed the LabMD Day Sheets and copied checks.

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)).

Response to Finding No. 420:

Complaint Counsel has no specific response.

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

Response to Finding No. 421:

To the extent the proposed finding implies Mr. Kam's testimony establishes that no consumers were harmed, it is misleading and irrelevant. Mr. Kam clarified that because there was no consumer notification in the case of consumers whose Personal Information was contained in the 1718 File, those consumers would have no way of knowing that any harm was connected with this case. (Kam, Tr. 532-533). The consumer injury component of Section 5's unfairness test is satisfied when security practices are likely to cause injury. (CCCL ¶¶ 12, 24-27). The proposed finding is also misleading to the extent it implies that victims of LabMD's disclosures and practices would necessarily be identifiable. (*See* CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer

to know which company was the source of the information that was then used to harm them, when a consumer does experience a harm.")).

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)).

Response to Finding No. 422:

The Court should disregard the proposed finding, because it is not supported by the citation to the record, and misleading. (*Compare* CX0742 (Kam Report) at 16, 21, *with* CCFF ¶¶ 1684-1692 (§ 8.3.4.1.1 Unauthorized Disclosure of CPT Codes Revealing Sensitive Conditions is Likely to Cause Harm), ¶¶ 1695-1697 (§ 8.3.4.1.2 There is a Significant Risk of Consumer Reputational Harm Due to the Unauthorized Disclosure of the CPT Codes), ¶¶ 1700-1701 (§ 8.3.4.1.3 Reputational Harm to Consumers May be Ongoing Because Once Health Information is Disclosed, it is Impossible to Restore a Consumer's Privacy), ¶¶ 1708-1711 (§ 8.3.4.3 With No Notification of Unauthorized Disclosure, No Mitigation of Harm is Possible)).

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)).

Response to Finding No. 423:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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)).

Response to Finding No. 424:

The Court should disregard the proposed finding, because it is not supported by the citation to the record, and irrelevant. Rather than cite specific pages or portions of evidence to

support its position, LabMD has improperly cited to the entirety of Mr. Kam's deposition testimony, expert report, and hearing testimony. Mr. Kam was not offered as an expert on computer network security.

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)).

Response to Finding No. 425:

The Court should disregard the proposed finding because it is not supported by the citations to the record, and irrelevant. Rather than cite specific pages or portions of evidence to support its position, LabMD has improperly cited to the entirety of Mr. Kam's deposition testimony, expert report, and hearing testimony. Mr. Kam was not offered as an expert on computer network security.

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

Response to Finding No. 426:

To the extent that the proposed finding asserts that LabMD's inadequate security practices did not injure consumers, the proposed finding is misleading and irrelevant. Mr. Kam clarified that because there was no consumer notification in the case of consumers whose Personal Information was contained in the 1718 File, those consumers would have no way of knowing that any harm was connected with this case. (Kam, Tr. 532-533; *see also* CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer to know which company was the source of the information that was then

used to harm them, when a consumer does experience a harm.")). Furthermore, the consumer injury component of Section 5's unfairness test is satisfied when security practices are likely to cause injury. (CCCL ¶¶ 12, 24-27).

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

Response to Finding No. 427:

The proposed finding is misleading and irrelevant. (CCRRFF ¶ 421 (addressing identical Proposed Finding 421)).

K. Jim Van Dyke

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)).

Response to Finding No. 428:

Complaint Counsel has no specific response.

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

Response to Finding No. 429:

The Court should disregard the proposed finding, because it is not supported by the citations to the record. Furthermore, the proposed finding is irrelevant because Mr. Van Dyke was not offered as an expert of computer network security, and Complaint Counsel's choices are not evidence.

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].

Response to Finding No. 430:

The Court should disregard the proposed finding, because it is not supported by the citations to the record, and irrelevant. Rather than cite specific pages or portions of evidence to support its position, LabMD has improperly cited to the entirety of Mr. Van Dyke's deposition testimony, Mr. Van Dyke's opening expert report, and Mr. Van Dyke's hearing testimony. Mr. Van Dyke was not offered as an expert of computer network security.

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)).

Response to Finding No. 431:

The proposed finding is irrelevant. Mr. Van Dyke was not offered as an expert of computer network security. In addition, the proposed finding misquotes Mr. Van Dyke's report. (CX0741 (Van Dyke Report) at 2 ("In rendering my expert opinions in this case, I have assumed that LabMD failed to provide reasonable and appropriate *security* for the personally identifiable information maintained on its computer networks.") (emphasis added)).

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).

Response to Finding No. 432:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 433:

The proposed finding is misleading. The full text of the cited portion of Mr. Van Dyke's expert report states as follows (with footnotes omitted):

> It is my opinion that LabMD's failure to provide reasonable and appropriate security for these categories of information places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of what is commonly called "identity theft" (also referred to as identity fraud, for the purposes of Javelin research). This includes the identity fraud subtypes, including new account fraud (NAF), existing non-card fraud (ENCF), existing card fraud (ECF), and medical identity fraud.

(CX0741 (Van Dyke Report) at 3).

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

Response to Finding No. 434:

The proposed finding is misleading and irrelevant. Mr. Van Dyke based his analysis of the facts in this case primarily on Javelin's nationally representative Identity (ID) Fraud Survey, which is fielded annually. (CCFF ¶ 27). The 2014 Identity Fraud report is based on the 2013 Javelin Identity Fraud Survey. (CCFF ¶ 27). In his analysis, Mr. Van Dyke looked at the portion of people who had their Social Security Number (SSN) exposed in the Javelin study, and compared that to the total quantity of LabMD's consumers who had their personally identifiable information, including their SSN and other elements of Personal Information, exposed. (CCFF ¶ 28). Mr. Van Dyke used the 2014 Identity Fraud report (based on the 2013 ID Fraud Survey) for his harm analysis of consumers affected by the Sacramento Day Sheets because those consumers were notified of the unauthorized disclosure of their Personal Information in March 2013. (CCFF ¶ 36).

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

Response to Finding No. 435:

The proposed finding is misleading and irrelevant. The proposed finding mischaracterizes Mr. Van Dyke's testimony and experience. Mr. James Van Dyke is a leader in

independent research on customer-related security, fraud, payments, and electronic financial services. (CCFF ¶ 22). He is founder and president of Javelin Strategy & Research (Javelin), which provides strategic insights into customer transactions. (CCFF ¶ 22). He leads the publication of the most rigorous annual, nationally representative victim study of identity crimes in the United States. (CCFF ¶ 22). Mr. Van Dyke makes frequent presentations on secure personal financial management and identity fraud and payments and security, to groups including the U.S. House of Representatives, Federal Reserve Bank gatherings, and the RSA Security Conference, in addition to being a public commentator in print and broadcast media. (CCFF ¶ 23). Mr. Van Dyke was not offered as an expert of computer network security.

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.").

Response to Finding No. 436:

Complaint Counsel has no specific response.

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.")).

Response to Finding No. 437:

Complaint Counsel has no specific response.

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.")).

Response to Finding No. 438:

The proposed finding is misleading. Contrary to LabMD's assertions, Mr. Van Dyke's opinions are based on a reliable methodology that he applied to the facts of this case.[13] Indeed, Mr. Van Dyke testified at length regarding the methodology used in forming his opinions, demonstrating that it is reliable and will assist the Court. (CCFF ¶¶ 30-31, 33-34, 36; Van Dyke, Tr. 601-611, 617-632). Among the many steps taken in forming his opinions, Mr. Van Dyke looked at the portion of people who had their Social Security Number (SSN) exposed in Javelin's nationally representative Identity (ID) Fraud Survey conducted in 2013. (CCFF ¶ 28).[14] Mr. Van Dyke then compared those figures to the total quantity of LabMD's consumers who had their personally identifiable information, including their SSNs and other elements of Personal Information, exposed. (CCFF ¶ 28). In doing so, Mr. Van Dyke was able to quantify both the incidence rate and financial impact of identity fraud that was likely to occur as a direct result of exposure of consumer personally identifiable information (PII) by LabMD. (CCFF ¶¶ 1736-1739; Van Dyke, Tr. 601-602). The calculations of the incidence rates as applied to the

[13] Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. (*See* CCRRFF ¶ 395).

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

LabMD-specific disclosures are supplied in Mr. Van Dyke's report and are supported by the accompanying spreadsheets. (CX0741 (Van Dyke Report) at 97-102).

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)).

Response to Finding No. 439:

The Court should disregard the proposed finding because it is not supported by the citation to the record.

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.")).

Response to Finding No. 440:

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

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.")).

Response to Finding No. 441:

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

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.")).

Response to Finding No. 442:

The proposed finding is irrelevant. Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. It is also misleading. As Mr. Van Dyke has explained, based on the survey data he has fielded for 10 years, the exact profile of a recipient of unauthorized information is not important for predicting in a statistically significant manner what is likely to occur next. (Van Dyke, Tr. 734). Rather, the single overriding factor for purposes of calculating fraud impacts is whether the individual who had access was authorized to receive the information. (Van Dyke, Tr. 734). Moreover, Mr. Van Dyke testified that he specifically considered whether the Day Sheets were "in the hands of

unauthorized parties" and he was aware that those documents "were found in the possession of individuals that have pleaded no contest to identity theft." (Van Dyke, Tr. 645-646; *see also* CCFF ¶¶ 1413-1458).

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.").

Response to Finding No. 443:

The proposed finding is misleading. As Mr. Van Dyke testified, the twelve-month period of time covered in the 2013 Javelin Identity Fraud Survey properly sets forth a snapshot that captures what frauds breach victims experienced. (Van Dyke, Tr. 740). Based on that data, Mr. Van Dyke provided reliable opinions quantifying the amount of likely out-of-pocket costs and hours spent to resolve fraud likely to occur within a twelve month period for individuals impacted by unauthorized disclosure of the Day Sheets. (Van Dyke, Tr. 691-692).

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]).

Response to Finding No. 444:

The proposed finding is misleading. Mr. Van Dyke based his opinions on the facts of the case, information documented in his literature review, materials provided to him by Complaint Counsel, and his experience and professional qualifications. (CCFF ¶ 25). Mr. Van Dyke based his analysis of the facts in this case primarily on Javelin's nationally representative Identity (ID) Fraud Survey, which is fielded annually. (CCFF ¶ 27). The 2014 Identity Fraud report is based

on the 2013 Javelin Identity Fraud Survey. (CCFF ¶ 27). Longitudinal comparisons of data from the respective Identity Fraud surveys, which have included data from more than 50,000 respondents over time, are used to identify consumer fraud trends over time. (CX0741 (Van Dyke Report) at 4). Mr. Van Dyke cited and relied on survey data from multiple years. (CX0741 (Van Dyke Report) at 8 (Fig. 1) (showing data from surveys in October 2010-2013); at 14 (Fig. 4) (same); at 37-39 (Attachment 1, Fig. 3-8) (same)).

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)).

Response to Finding No. 445:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 446:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Mr. Van Dyke cited and relied on survey data from multiple years. (*See* CCRRFF ¶ 444). Furthermore, the proposed finding is irrelevant because Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703 (including testimony regarding identifying the 1718 File in 2013), or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony.

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)).

Response to Finding No. 447:

Complaint Counsel has no specific response.

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. (CX 0742 (Van Dyke, [redacted]).

Response to Finding No. 448:

The Court should disregard the proposed finding because it is not supported by the citation to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. Furthermore, to the extent the proposed finding asserts that there was a consistent decrease in the total one year fraud amount over the stated time period, it is not supported by Figure 3 of Attachment 1 to Mr. Van Dyke's report, entitled "Identity Fraud Overall Metrics by Survey Year," which includes, among others, a category entitled "Total one year fraud amount (in billions)," the value of which did not consistently decrease and instead fluctuated for the Survey Report years 2006 through 2012. (CX0741 (Van Dyke Report) at 37 (Attachment 1, Fig. 3)).

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. (CX 0742 (Van Dyke, [redacted]).

Response to Finding No. 449:

The Court should disregard the proposed finding because it is not supported by the citation to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. Otherwise, Complaint Counsel has no specific response.

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. (CX0742 (Van Dyke, [redacted]).

Response to Finding No. 450:

The Court should disregard the proposed finding because it is not supported by the citation to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. Otherwise, Complaint Counsel has no specific response.

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. (CX0742 (Van Dyke, [redacted]).

Response to Finding No. 451:

The Court should disregard the proposed finding because it is not supported by the citation to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. Furthermore, to the extent the proposed finding asserts that there was a consistent decrease in the mean consumer cost amount over the stated time period, it is not supported by Figure 3 of Attachment 1 to Mr. Van Dyke's report. On the contrary, the mean consumer cost increased from 2011 to 2012, from $354 to $365. Otherwise, Complaint Counsel has no specific response.

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. (CX0742 (Van Dyke, [redacted]).

Response to Finding No. 452:

The Court should disregard the proposed finding because it is not supported by the citation to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. Otherwise, Complaint Counsel has no specific response.

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)); (CX0742 (Van Dyke, [redacted]).

Response to Finding No. 453:

The Court should disregard the proposed finding because it provides an opinion and does not state any fact, and is not supported by the citations to the record: CX0742 is Mr. Kam's Report; Mr. Van Dyke's Report is CX0741. The proposed finding is also not supported by the citations to the record as to the time period addressed by Mr. Van Dyke's opinion. On the contrary, Mr. Van Dyke's opinion is not time-limited. (*See* CX0741 (Van Dyke Report) at 2 (describing assumptions and what Van Dyke was asked to do).[15] Furthermore, the proposed finding is not supported by the citation to the record because the cited figure from Mr. Van Dyke's report does not contradict or belie his report or opinions. On the contrary, Mr. Van Dyke's report demonstrates a significantly high risk of becoming a victim of identity fraud and/or medical identity theft/fraud for consumers whose personal information was disclosed by LabMD and consumers for whom LabMD failed to provide reasonable security for their personal information that it maintained and consumers . Mr. Van Dyke based his analysis of the facts in this case primarily on Javelin's nationally representative Identity (ID) Fraud Survey, which is fielded annually. (CCFF ¶ 27). The 2014 Identity Fraud report is based on the 2013 Javelin Identity Fraud Survey. (CCFF ¶ 27). Longitudinal comparisons of data from the respective Identity Fraud surveys, which have included data from more than 50,000 respondents over time, are used to identify consumer fraud trends over time. (CX 0741 (Van Dyke Report) at 4). Mr. Van Dyke cited and relied on survey data from multiple years. (CX 0741 (Van Dyke Report) at 8 (Fig. 1) (showing data from surveys in October 2010-2013); at 14 (Fig. 4) (same); at 37-39 (Attachment 1, Fig. 3-8) (same)).

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

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)).

Response to Finding No. 454:

To the extent it asserts that the Ponemon Survey was financed by Mr. Kam's company, the Court should disregard the proposed finding because it is not supported by the citation to the record. The proposed finding is also misleading to the extent it asserts that Mr. Van Dyke relied primarily on the Ponemon Survey. The Survey is included in a list of research supporting Mr. Van Dyke's opinion. (CX0741 (Van Dyke Report) at 18). Mr. Van Dyke based his opinions on the facts of the case, information documented in his literature review, materials provided to him by Complaint Counsel, and his experience and professional qualifications. (CCFF ¶ 25). Mr. Van Dyke based his analysis of the facts in this case primarily on Javelin's nationally representative Identity (ID) Fraud Survey, which is fielded annually. (CCFF ¶ 27). The 2014 Identity Fraud report is based on the 2013 Javelin Identity Fraud Survey. (CCFF ¶ 27). Otherwise, Complaint Counsel has no specific response.

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)).

Response to Finding No. 455:

The proposed finding is misleading and irrelevant. As Mr. Van Dyke explained, his approach for forming opinions in this case was based on ten years of experience conducting a methodologically rigorous survey of more than 5,000 people with the assistance of statistical experts. (Van Dyke, Tr. 730-731). The resulting opinions quantify likely harm to consumers resulting from LabMD's unauthorized disclosures within a twelve-month period. (Van Dyke, Tr. 687, 691-692). Mr. Van Dyke further explained that medical identity fraud has the potential to

be a lifelong threat for consumers affected by LabMD's unauthorized disclosures, such that consumer injury may occur well into the future. (CX0741 (Van Dyke Report) at 14). The types of personally identifiable information (PII) that rarely change can be used fraudulently for extended periods of time once compromised, placing consumers at risk of injury indefinitely. (CCFF ¶ 1566). To the extent that the proposed finding asserts that LabMD's inadequate security practices did not harm consumers, the proposed finding is misleading and irrelevant. The consumer injury component of Section 5's unfairness test is satisfied when security practices are likely to cause substantial injury. (CCCL ¶¶ 12, 24-27). The proposed finding is also misleading to the extent it implies that victims of LabMD's disclosures and practices would necessarily be identifiable. (CCFF ¶ 414).

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).

Response to Finding No. 456:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, merely provides an opinion and does not state any fact, and is not supported by the citation to the record. As Mr. Van Dyke explained, his approach for forming opinions in this case was based on ten years of experience conducting a methodologically rigorous survey of more than 5,000 people with the assistance of statistical experts. (Van Dyke,

Tr. 730-731). The resulting opinions quantify likely harm to consumers resulting from LabMD's unauthorized disclosures within a twelve-month period. (Van Dyke, Tr. 687, 691-692). Mr. Van Dyke further explained that medical identity fraud has the potential to be a lifelong threat for consumers affected by LabMD's unauthorized disclosures, such that consumer injury may occur well into the future. (CX0741 (Van Dyke Report) at 14). The types of personally identifiable information (PII) that rarely change can be used fraudulently for extended periods of time once compromised, placing consumers at risk of injury indefinitely. (CCFF ¶ 1566).

Furthermore, the assertion that "victims of identity theft from the 1718 File and the Day Sheets do not exist" is contradicted by the weight of the evidence. (*See, e.g.*, CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer to know which company was the source of the information that was then used to harm them, when a consumer does experience a harm.")).

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.").

Response to Finding No. 457:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, merely provides an opinion and does not state any fact, and is not supported by the citations to the record. As Mr. Van Dyke explained, his approach for forming

opinions in this case was based on ten years of experience conducting a methodologically rigorous survey of more than 5,000 people with the assistance of statistical experts. (Van Dyke, Tr. 730-731). The resulting opinions quantify likely harm to consumers resulting from LabMD's unauthorized disclosures within a twelve-month period. (Van Dyke, Tr. 687, 691-692). Mr. Van Dyke further explained that medical identity fraud has the potential to be a lifelong threat for consumers affected by LabMD's unauthorized disclosures, such that consumer injury may occur well into the future. (CX0741 (Van Dyke Report) at 14). The types of personally identifiable information (PII) that rarely change can be used fraudulently for extended periods of time once compromised, placing consumers at risk of injury indefinitely. (CCFF ¶ 1566).

Furthermore, to the extent the proposed finding asserts that "none of the individuals notified by LabMD that their PII (Personal Identifying Information) had been disclosed to unauthorized persons became victims of identity fraud" is contradicted by the weight of the evidence. (*See, e.g.*, CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer to know which company was the source of the information that was then used to harm them, when a consumer does experience a harm.")).

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)).

Response to Finding No. 458:

The proposed finding is irrelevant. Mr. Van Dyke was not offered as an expert on computer network security.

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).

Response to Finding No. 459:

Complaint Counsel has no specific response.

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.").

Response to Finding No. 460:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, and merely provides an opinion and does not state any fact. In addition, the Court should disregard the proposed finding because it is not supported by the citations to the record, and is misleading and irrelevant. As Mr. Van Dyke explained, his approach for forming opinions in this case was based on ten years of experience conducting a methodologically rigorous survey of more than 5,000 people with the assistance of statistical experts. (Van Dyke, Tr. 730-31). Mr. Van Dyke explained that statisticians working at Javelin do the type of cross-tabulation Mr. Van Dyke testified about. (Van Dyke, Tr. 674).

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. . . .").

Response to Finding No. 461:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, merely provides an opinion and does not state any fact, and is not supported by the citation to the record. The proposed finding also mischaracterizes Mr. Van

Dyke's testimony by selectively excerpting it. His description of cross-tabulation is consistent when his entire answers are read:

> 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. So an example might be, you might ask somebody a battery of questions: Did you visit Washington, D.C. on Wednesday of last week? And did you have apple pie when you were on a visit somewhere on Wednesday of last week? And if a person answered yes to those, you could do a cross-tabulation to say X percent of people who were in Washington, D.C. last week had apple pie while they were in Washington, D.C.**

(Van Dyke, Tr. 587).

> Q. Mr. Van Dyke, what is cross-tabulation? How would you define that?
> **A. Yeah. Cross-tabulation is -- I used the kind of simplistic example earlier just to put something that sounds complex in everyday terms -- when we ask individuals a wide variety of questions, as our surveys often do, comparing the results of individuals who responded in a particular way to one question to those individuals -- it might be the same individuals or different individuals -- who answered in a particular way to another set of questions. So the example I gave earlier was individuals who said they were in Washington, D.C. last Wednesday and individuals who said, I had apple pie last Wednesday. And we compare one to the other and say, well, there's almost like an overlapping circle, so many people had apple pie in Washington, D.C. last Wednesday because of the overlap or the comparison.**

(Van Dyke, Tr. 650).

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)).

Response to Finding No. 462:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, merely provides an opinion and does not state any fact, and is not supported by the citations to the record. The proposed finding also mischaracterizes Mr. Van Dyke's testimony.

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.").

Response to Finding No. 463:

Complaint Counsel has no specific response.

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).

Response to Finding No. 464:

Complaint Counsel has no specific response.

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).

Response to Finding No. 465:

The Court should disregard the proposed finding because it is not supported by the citation to the record because it mischaracterizes Mr. Van Dyke's testimony. Mr. Van Dyke agreed with Respondent's counsel's description of how the survey data was cross-tabulated and then overlaid on the information from the 1718 File, but did not agree that the process was extrapolation. (Van Dyke, Tr. 676-77).

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

Response to Finding No. 466:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Furthermore, contrary to LabMD's assertions, Mr. Van Dyke's opinions are based on a reliable methodology that he applied to the facts of this case. Indeed, Mr. Van Dyke testified at length regarding the methodology used in forming his opinions, demonstrating that it is reliable and will assist the Court. (CCFF ¶¶ 30-31, 33-34, 36; Van Dyke, Tr. 601-11, 617-32). Among the many steps taken in forming his opinions, Mr. Van Dyke looked at the portion of people who had their Social Security Number (SSN) exposed in Javelin's nationally representative Identity (ID) Fraud Survey conducted in 2013. (CCFF ¶ 27). Mr. Van Dyke then compared those figures to the total quantity of LabMD's consumers who had their personally identifiable information, including their SSNs and other elements of Personal Information, exposed. (CCFF ¶ 28). In doing so, Mr. Van Dyke was able to quantify both the incidence rate and financial impact of identity fraud that was likely to occur as a direct result of exposure of consumer personally identifiable information (PII) by LabMD. (CCFF ¶¶ 1736-1739; Van Dyke, Tr. 601-02). The calculations of the incidence rates as applied to the LabMD-specific disclosures are supplied in Mr. Van Dyke's report and are supported by the accompanying spreadsheets. (CX0741 (Van Dyke Report) at 97-102)).

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

Response to Finding No. 467:

The proposed finding is misleading. As Mr. Van Dyke has explained, based on the survey data he has fielded for 10 years, the exact profile of a recipient of unauthorized

information is not important for predicting in a statistically significant manner what is likely to occur next. (Van Dyke, Tr. 734). Rather, the single overriding factor for purposes of calculating fraud impacts is whether the individual who had access was authorized to receive the information. (Van Dyke, Tr. 734). Moreover, Mr. Van Dyke testified that he specifically considered whether the Day Sheets were "in the hands of unauthorized parties" and he was aware that those documents "were found in the possession of individuals that have pleaded no contest to identity theft." (Van Dyke, Tr. 645-646; CCFF ¶¶ 1413-1458).

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)).

Response to Finding No. 468:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Mr. Van Dyke did not testify that he assumed the same amount of damage would occur. (RX523 (Van Dyke, Dep. at 41-42)). He testified that the when and how long the file was exposed did not figure into his analysis. (RX523 (Van Dyke, Dep. at 41-42)). However, Respondent has cited to no evidence to establish that the significance of the length of time the file was available on a peer to peer network.

The proposed finding is also misleading. As Mr. Van Dyke testified, the twelve-month period of time covered in the 2013 Javelin Identity Fraud Survey properly sets forth a snapshot of what frauds the breach victims experienced. (Van Dyke, Tr. 740). Based on that data, Mr. Van Dyke provided reliable opinions quantifying the amount of likely out-of-pocket costs and hours spent to resolve fraud likely to occur within a twelve month period for individuals impacted by unauthorized disclosure of the Day Sheets. (CX0741 (Van Dyke Report); Van Dyke, Tr. 740).

L. Professor Shields

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

Response to Finding No. 469:

The proposed finding is misleading to the extent it implies that Complaint Counsel's rebuttal expert Clay Shields is not an expert on P2P networks and peer-to-peer clients such as LimeWire. Professor Shields is an expert on these topics. To the extent the proposed finding is limited to the experts Complaint Counsel offered in its affirmative case, Complaint Counsel has no specific response.

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

Response to Finding No. 470:

Complaint Counsel has no specific response.

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).

Response to Finding No. 471:

Complaint Counsel has no specific response.

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).

Response to Finding No. 472:

The proposed finding is misleading. Professor Shields did not attempt to locate the 1718 File. (Shields, Tr. 892).

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

Response to Finding No. 473:

The proposed finding is misleading. Professor Shields has extensive experience with the Gnutella network, for which LimeWire is a client. (CX0738 (Shields Rebuttal Report) ¶ 9; Shields, Tr. 893; CCFF ¶ 47). There is very little difference between various Gnutella clients. (Shields, Tr. 893; CX0738 (Shields Rebuttal Report) ¶¶ 13-14 (explaining that analysis would apply equally to any Gnutella client)).

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).

Response to Finding No. 474:

Complaint Counsel has no specific response.

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).

Response to Finding No. 475:

The proposed finding is misleading and irrelevant. Mr. Boback's deposition was one document out of many that Professor Shields reviewed. (Shields, Tr. 905-07; CX0738 (Shields Rebuttal Report) Appendix B (listing all materials Prof. Shields considered in preparing his report)). Respondent points to no evidence that Professor Shields "based" his report on Mr. Boback's testimony, or even considered it particularly important. Professor Shields "assumed" that the 1718 file was available only insofar as he was asked to respond to Mr. Fisk's report and its conclusions on how the 1718 File was found on the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶ 2). There is overwhelming evidence that the 1718 File was available on the Gnutella network from the LabMD computer used by its billing manager. (CCFF ¶¶ 1363-1372).

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

Response to Finding No. 476:

Complaint Counsel has no specific response.

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

Response to Finding No. 477:

The proposed finding is misleading. Professor Shields compared finding a particular file on a P2P network as being like a lottery because of the large number of lottery players and P2P users. Given the huge number of lottery players and P2P users performing searches, it is a near certainty that someone will win the lottery and one or more of the P2P users will find a file even if it is unlikely that any given lottery ticket will win or that any given P2P search will locate the file. (CX0738 (Shields Rebuttal Report) ¶¶ 59-61, Shields, Tr. 873-74).

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).

Response to Finding No. 478:

Complaint Counsel has no specific response.

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)).

Response to Finding No. 479:

Complaint Counsel has no specific response.

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).

Response to Finding No. 480:

To the extent the proposed finding asserts that Complaint Counsel introduced evidence that LabMD's data security practices caused or are likely to cause substantial injury to consumers or competition, Complaint Counsel has no specific response. To the extent the proposed finding is used to assert the opposite: that Complaint Counsel *has not* introduced any such evidence, the proposed finding is misleading and contradicted by the weight of the evidence. Complaint Counsel's burden is "to prove by a preponderance of evidence that LabMD's practices are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." (CCCL ¶ 3 (quoting JX0001-A at 3)). Complaint Counsel has shown by a preponderance of the evidence that LabMD's failure to employ reasonable security practices "caused, or is likely to cause, substantial injury to consumers . . . ." (Compl. ¶ 22; CCFF ¶¶ 1472-1798).

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).

Response to Finding No. 481:

This finding is misleading to the extent it suggests that Complaint Counsel must show current or future injury to show that conduct violated Section 5. The evidence supports a finding that LabMD's past conduct in this case was unfair and unlawful. Complaint Counsel need only show that LabMD's acts or practices "caused, or were likely to cause, substantial injury to consumers." (CCRRCL ¶¶ 56-57).

482. Although recurrence is not required for LabMD's practices to have violated Section 5, to the extent the proposed finding relates to appropriateness of entry of the Notice Order, Complaint Counsel has shown that there is sufficient danger of LabMD's unreasonable security

practices continuing to warrant imposition of the Notice Order. (CCFF ¶ 513; CCCL ¶¶ 57-71). 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).

Response to Finding No. 482:

The Court should disregard the proposed finding because it calls for a legal conclusion, not a fact. To the extent the proposed finding argues that the 1718 File was not available for sharing through LimeWire from a computer used by LabMD's billing manager after 2008, Complaint Counsel has no specific response. To the extent the proposed finding argues that the evidence shows that the 1718 File was never obtained by anyone other than Tiversa, Johnson, Dartmouth, and Commission staff, it is misleading and not supported by the citations to the record. However, Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony. (*See* CCRRFF ¶ 395).

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)).

Response to Finding No. 483:

To the extent the proposed finding asserts that the 1718 File was disclosed to Johnson and Dartmouth, the Court should disregard it because it is not supported by the citations to the record. The proposed finding is also misleading to the extent it asserts that the 1718 File was "taken," rather than downloaded from a computer sharing it. The 1718 File was shared by LabMD's billing manager through LimeWire on a computer used by LabMD's billing manager. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4; CCFF ¶¶ 1354-1406). To the extent the proposed finding argues that Tiversa downloaded the 1718 File from a LabMD

computer on February 25, 2008, whence it was shared, Complaint Counsel has no specific response.

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)).

Response to Finding No. 485:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Moreover, the proposed finding is contradicted by the weight of the evidence. The evidence in the record does not prove that the 1718 File was not obtained by other parties. (*See, e.g.*, Wallace, Tr. 1435 (testifying that Tiversa's stated capability to record searches happening on P2P networks did not exist); CCFF ¶¶ 1229-1230 (difficult or impossible to remove files from a P2P network), ¶¶ 1259-1266 (searches of P2P network may fail to locate a particular file), ¶ 1393 (1718 File could be discovered by anyone looking for it)). Notwithstanding, evidence of "'actual, completed economic harms' [is] not necessary to substantiate that [LabMD's] data security activities caused or likely caused consumer injury, and thus constituted 'unfair . . . acts or practices.'" Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014).

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)).

Response to Finding No. 486:

The Court should disregard the proposed finding because it is not supported by the citations to the record. (*See* CCFF ¶¶ 660-696 (§ 4.3.2.3 LabMD's Manual Inspections Could

Not Reliably Detect Security Risks) (finding that LabMD did not detect presence of LimeWire installed on LabMD computer since 2006)).

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).

Response to Finding No. 484:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. (*See, e.g.*, CCFF ¶¶ 1578-1580 (it may take years for consumers to learn of misuses and identity crimes), ¶¶ 1704-1705 (LabMD did not notify consumers whose Personal Information appeared in the 1718 File that their Personal Information had been made publicly available), ¶ 1774 ("It is therefore difficult for a consumer to know which company was the source of the information that was then used to harm them, when a consumer does experience a harm.")).

485a. 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).

Response to Finding No. 485a:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. (*See, e.g.*, CCFF ¶¶ 1763-1770 (notification to Sacramento Consumers does not eliminate all risk of harm; consumers cannot avoid all harms through notification), ¶¶ 1472-1639 (identity theft, medical identity theft, and medical identity fraud)). Moreover, most victims of LabMD's exposure of sensitive Personal Information have not yet received notice of that exposure. (CCFF ¶ 1704).

486a. 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)).

Response to Finding No. 486a:

The proposed finding is misleading to the extent it suggests that Complaint Counsel must show current or future injury to show that conduct violated Section 5. The evidence supports a finding that LabMD's past conduct in this case was unfair and unlawful. Complaint Counsel need only show that LabMD's acts or practices "caused, or were likely to cause, substantial injury to consumers." (*See* CCRRCL ¶¶ 56-57).

Although recurrence is not required for LabMD's practices to have violated Section 5, to the extent the proposed finding relates to appropriateness of entry of the Notice Order, Complaint Counsel has shown that there is sufficient danger of LabMD's unreasonable security practices continuing to warrant imposition of the Notice Order. (CCFF ¶ 513; CCCL ¶¶ 57-71).

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).

Response to Finding No. 487:

The proposed finding is incorrect. Complaint Counsel did in fact introduce evidence regarding the allegation in ¶ 4 of the Complaint. This evidence shows that consumers pay LabMD's charges with credit cards, debit cards, or personal checks. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 6, Adm. 29; CX0706 (Brown, Dep. at 39-40); CX0765 (LabMD's Resps. to Second Set of Discovery) at 8, Resp. to Interrog. 13).

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)).

Response to Finding No. 489:

The Court should disregard the proposed finding because it is not supported by the citations to the record. In addition, Complaint Counsel has introduced evidence regarding the allegation in ¶ 6 of the Complaint. Specifically, in connection with performing tests, LabMD has collected and continues to maintain consumers' Personal Information. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 3; CCFF ¶¶ 72-161). Furthermore, LabMD neither deletes nor destroys Personal Information of consumers, but maintains it indefinitely. (CX0710-A (Daugherty, LabMD Designee, Dep. at 60, 215-16, 220-21)).

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

Response to Finding No. 490:

The proposed finding is contradicted by the weight of the evidence. LabMD continues to operate a computer network consisting of switches, routers, servers, workstation computers, printers, a scanner, and an Internet connection at Mr. Daugherty's residence, as well as a workstation at a condominium that can remotely connect to a server at the private residence network and a printer for the condominium workstation. (CCFF ¶¶ 251-260 (§ 4.7.4 Internal Network from January 2014 to Present)). In addition, LabMD has no intention of dissolving as a Georgia corporation, retains the personal information of over 750,000 consumers, and intends to employ the same unreasonable policies and procedures to Personal Information in its possession as it employed in the past. (CCCL ¶¶ 60-64).

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)).

Response to Finding No. 491:

The Court should disregard this proposed finding because it is not supported by the citation to the record. Further, whether or not LabMD's billing department actually uses computer networks to generate or access documents related to processing copies of consumer checks is not as significant as the fact that LabMD retained copies of checks and money orders containing consumers' account numbers, bank routing numbers, signatures, and often addresses and phone numbers. (CX0716 (Harris, Dep. at 23, 27); CX0706 (Brown, Dep. at 28-29, 31); CX0715-A (Gilbreth, Dep. at 50-51); CX0088 (*in camera*)[16] (LabMD Copied Checks) at 1-10). The billing department posted the payment to the patient's account and filed the copy of the check or money order in unlocked file cabinets. (CX0716 (Harris, Dep. at 24-25, 27); CX0714-A ([Fmr. LabMD Empl.], Dep. at 62-63, 70-71)). In fact, LabMD continues to maintain copies of hundreds of personal checks (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 7, Adm. 32), and has never destroyed any of those copies. (CX0733 (Boyle, IHT at 46); CX0716 (Harris, Dep. at 25); *see also* (CX0706 (Brown, Dep. at 31)).

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).

Response to Finding No. 492:

The proposed finding is incorrect. Complaint Counsel did introduce 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

[16] Complaint Counsel has not marked as nonpublic its responses to Respondent's proposed findings of fact that cite to *in camera* exhibits where (1) the exhibit has been granted *in camera* status due to the inclusion of Sensitive Personal Information as defined in Rule 3.45(b) and (2) the citation is to the existence or nature of the exhibit, or to general information about the exhibit as a whole, rather than to specific Sensitive Personal Information contained therein.

computer networks." (*See* CCFF ¶¶ 382-1110 (§ 4 LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Network), ¶¶ 1113-1185 (§ 5 LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures), ¶¶ 1354-1469 (§ 7 Security Incidents at LabMD), ¶¶ 1472-1798 (§ 8 LabMD's Data Security Practices Caused or are Likely to Cause Substantial Injury to Consumers That is Not Reasonably Avoidable by the Consumers Themselves and Are Not Outweighed by Countervailing Benefits to Consumers or Competition)).

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)).

Response to Finding No. 493:

The Court should disregard the proposed finding because it is not supported by the citations to the record and other cited sources. The cited sources, including the expert report of

Respondent's expert, Mr. Fisk, do not describe any readily available measures LabMD has taken to identify commonly known or reasonably foreseeable risks and vulnerabilities on its networks. (*See* CCRRFF ¶¶ 279-286). Furthermore, Complaint Counsel has proven by a preponderance of the evidence that LabMD failed to employ readily available measures to identify commonly known or reasonably foreseeable risks and vulnerabilities on its networks. (CCFF ¶¶ 524-808).

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)).

Response to Finding No. 494:

The Court should disregard the proposed finding to the extent that LabMD has cited its expert Mr. Fisk in support of a factual proposition, in violation of the Court's Order on Post-Trial Briefs.

Furthermore, the Court should disregard the proposed finding because it is not supported by the citations to the record. CX0005 does not reflect any authentication-related security measures, such as password policies, and do not support the proposed finding. Nor do RX075 through RX095, signed copies of an acknowledgement page of a policy, because they do not include any policy themselves. Likewise CX0001/RX071,[17] LabMD's Employee Handbook revised 2004, does not contain any information about authentication-related security measures, such as passwords. (*See, e.g.*, RX071 at 5 (confidentiality section does not address passwords), 7 (personal mail, e-mail, and phone calls section does not address passwords), 9 (security policy does not address passwords)). Similarly, CX0130, which consists of the first four pages of a

[17] Although RX071 appears at a different Bates range than CX0001, and was therefore not included in the parties' Duplicate CX and RX Exhibit Index, CX0001 and RX071 are both LabMD's Employee Handbook revised June 2004. They are identical except but for the Bates stamps and an additional blank page that appears in CX0001 at 22.

version of LabMD's handbook revised in October 2007 followed by 42 pages of employee signatures, does not contain any password-related policies. A complete copy of LabMD's handbook revised October 2007 is not in evidence.

Furthermore, the proposed finding is contradicted by the weight of the evidence. LabMD did not adopt and implement policies prohibiting employees from using weak passwords, (CCFF ¶¶ 909-916), did not have policies for strong passwords, (CCFF ¶¶ 919-931), did not have enforcement mechanisms to ensure its employees used reasonable password practices, (CCFF ¶¶ 934-942), did not prevent employees from using the same passwords for years (CCFF ¶¶ 954-957), did not prevent employees from sharing authentication credentials, (CCFF ¶¶ 960-963), and allowed weak passwords to be used on computers placed in physician-client offices (CCFF ¶¶ 974-983).

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).

Response to Finding No. 495:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Complaint Counsel has proven by a preponderance of the evidence that LabMD could have corrected its security failures at relatively low cost using readily available security measures. (CCFF ¶¶ 1115-1183).

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).

Response to Finding No. 496:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Complaint Counsel has proven by a preponderance of the evidence that consumers had no way of independently knowing about LabMD's security failures and could not reasonably avoid possible harms from such failures. Consumers needing medical tests did not know that LabMD would receive and test their specimens. (CCFF ¶¶ 1777-1782). Consumers could not have known what LabMD's data security practices were before their specimen was sent to LabMD for testing. (CCFF ¶¶ 1785-1787). LabMD did not routinely inform its physician-clients about its data management practices, did not provide details to those who inquired about them, and assured physician-clients that their data at LabMD was secure. (CCFF ¶¶ 1790-1795).

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)).

Response to Finding No. 497:

The Court should disregard the proposed finding because it attempts to state a legal conclusion. The Court should also disregard the proposed finding to the extent it consists of Respondent's representation of Complaint Counsel's evaluation of LabMD's HIPAA compliance, which is false and not supported by the citation to the record. Respondent's bald factual assertions in CX0679, its complaint against the Commission in the Northern District of Georgia seeking to enjoin this proceeding, were made without evidentiary support and do not prove any fact in issue in this proceeding. Respondent presented no evidence on its compliance with HIPAA, and in fact affirmatively declined to provide evidence on its HIPAA compliance. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating

that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

In any event, whether LabMD complied with HIPAA/HITECH data-security standards is irrelevant to this case because it must still comply with the FTC Act. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't Mot. for Summ. Decision at 5-6 (May 19, 2014). Indeed, LabMD has conceded that its compliance with HIPAA is irrelevant. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence")).

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

Response to Finding No. 498:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The adequacy of the HIPAA Breach Notification Rule – which sets forth circumstances under which companies must notify consumers of data breaches – is irrelevant to this case for two reasons. First, whether LabMD complied with any HIPAA/HITECH data-security standards is irrelevant, because it must still comply with the FTC Act. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12 (Jan. 16, 2014) (dismissing LabMD's argument that HHS has exclusive authority over HIPAA covered entities as "without merit," and noting that "nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act."); Comm'n Order Denying Resp't Mot. for Summ. Decision at 5-6 (May 19, 2014).

Second, this case is not about the adequacy of Respondent's breach notification, but about the adequacy of Respondent's data security.

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)).

Response to Finding No. 499:

The Court should disregard the proposed finding because it is contradicted by uncontroverted evidence in the record. The Commission issued warning concerning the risks of P2P software as early as July 2003. (*See* CCFF ¶¶ 1338-1351).

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).

Response to Finding No. 500:

The Court should disregard the proposed finding because it is contradicted by the weight of the evidence, and not supported by the citations to the record. Mr. Fisk's conclusion that a simple search of "insurance" would not have found the file, while correct, is irrelevant. There is overwhelming evidence that the 1718 File was available on the Gnutella network, including Mr. Wallace's testimony that he downloaded the 1718 File on a P2P network. (Wallace, Tr. 1342 (Mr. Wallace searched the P2P network "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"), 1371-72 (Mr. Wallace found the 1718 File using a "stand-alone desktop computer"; *see also* CCFF ¶¶ 1393-1396).

Further, there were many ways in which the 1718 File could have been found by a user of the Gnutella network. (CCFF ¶¶ 1240-1306; CX0738 (Shields Rebuttal Report) ¶¶ 50-99). Prof. Shields set forth these reasons in his report, showing that Mr. Fisk's conclusion was erroneous. (CX0738 (Shields Rebuttal Report) ¶¶ 50-99). Neither Respondent nor Mr. Fisk have presented any testimony or other evidence that suggests that any of the methods described by Prof. Shields would be ineffective.

498a. 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).

Response to Finding No. 498a:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. (*See* CCRRFF ¶ 485a (addressing substantively identical Proposed Conclusion ¶ 485a); CCRRCL ¶ 83). Moreover, most victims of LabMD's exposure of sensitive Personal Information have not yet received notice of that exposure. (CCFF ¶ 1704).

499a. 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).

Response to Finding No. 499a:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. (*See* CCFF ¶¶ 1224-1231).

500a. 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).

Response to Finding No. 500a:

The Court should disregard the proposed finding because it is not supported by the citations to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. (*See* CCFF ¶¶ 1316-1351).

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)).

Response to Finding No. 502:

The Court should disregard the proposed finding because it is contradicted by the weight of the evidence. The uncontroverted evidence in this proceeding is that the Commission issued warning concerning the risks of P2P software as early as July 2003. (*See* CCFF ¶¶ 1338-1351).

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).

Response to Finding No. 501:

The Court should disregard the proposed finding because it is not supported by the citation to the record. Furthermore, the proposed finding is contradicted by the weight of the evidence. There is overwhelming evidence that the 1718 File was available on the Gnutella network. (*See* CCRRFF ¶ 500 (addressing substantively identical Proposed Finding 500)).

502a. 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)).

Response to Finding No. 502a:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, and is a misstatement of the law. Knowledge is not an element of a Section 5 violation, and Complaint Counsel need not prove a knowing violation. 15 U.S.C. § 45.

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

Response to Finding No. 503:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact, and is a misstatement of the law. Serial violations are not an element of a Section 5 violation, and Complaint Counsel need not allege or prove serial violations. 15 U.S.C. § 45(n) (referring to "*an* act or practice" (emphasis added)).

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)).

Response to Finding No. 504:

The Court should disregard the proposed finding because it is not supported by the citation to the record. To the extent the proposed finding attempts to state a legal conclusion, the Court should reject the proposed finding because it is not supported by any legal authority. Respondent has not alleged at any stage of this process that it lacked notice of the complaint allegations against it, and, indeed, filed an answer to the paragraph of the Complaint it now complains of without raising any issues of notice or indefiniteness. (Ans. ¶ 10).

Complaint Counsel's complaint complies with Rule 3.11(b), which requires the complaint to recite the "legal authority and jurisdiction for institution of the proceeding" and contain "a clear and concise factual statement sufficient to inform . . . respondent with reasonable definiteness of the type of acts or practices alleged to be in violation of the law." 16 C.F.R. § 3.11(b). A complaint "need not . . . give[]" all the details "which [respondent] will need before he can mount a defense against its allegations. . . ." Order Denying Resp't's Mot. for More Definite Statement, *Diran M. Seropian, M.D.*, Docket No. 9248, 1991 WL 11000977, at *1 (F.T.C. July 3, 1991). A complaint gives notice of the charges against a respondent, and "details of the Commission's case will be revealed . . . during the discovery phase. . . ." *Id.* at *1. The Commission has already determined whether "'[T]he [Complaint] contains sufficient factual matter . . . to state a claim to relief that is plausible on its face,'" Comm'n Order Denying Resp't's Mot. to Dismiss at 3 (Jan. 16, 2014) (quoting *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2010), and declined to dismiss the complaint, *id.* at 19.

To the extent the proposed finding asserts that Respondent does not have fair notice, the Commission has disposed of that argument with regard to due process. Comm'n Order Denying Resp't's Mot. to Dismiss at 16-17 (Jan. 16, 2014).

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)).

Response to Finding No. 505:

To the extent the proposed finding asserts that the Complaint must name an individual complainant or identify harm to specific persons, or cite regulations for the terms it uses, it attempts to state a legal conclusion, not a fact. As a legal conclusion, the proposed conclusion is unsupported and a misstatement of law. The Commission is "empowered and directed to prevent . . . unfair or deceptive acts or practices in or affecting commerce," among others, without naming a complainant or alleging harm to a specific person, including practices that are "likely to cause substantial injury to consumers." 15 U.S.C. § 45(a)(2), (n). Likewise, the Commission is not required to allege regulations, guides, or standards where the Complaint alleges unfair acts or practices in violation of Section 5; the statutory definition of unfairness provides adequate notice. Comm'n Order Denying Resp't's Mot. to Dismiss at 16-17 (Jan. 16, 2014).

To the extent the proposed finding quotes the Complaint, Complaint Counsel has no specific response.

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)).

Response to Finding No. 506:

To the extent the proposed finding asserts that the Complaint must cite regulations or guidance, it attempts to state a legal conclusion, not a fact. As a legal conclusion, the proposed conclusion is unsupported and a misstatement of law. (*See* CCRRCL ¶¶ 89-90 (Respondent did

not lack fair notice) ¶¶ 51, 85 (Section 5(n) provides notice of what conduct is unfair, and unfairness is assessed under a reasonableness test)).

The Complaint sets forth LabMD's alleged failures to employ reasonable and appropriate data security and articulates how those acts or practices violate Section 5. (*See* Compl. ¶¶ 5-23).

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.").

Response to Finding No. 507:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. The cited testimony does not describe the efficiency of LabMD's process in relation to pre-existing or competing processes and the Court should disregard it as impermissible expert testimony.

The Court should disregard the proposed finding to the extent it contains a legal conclusion regarding whether consumer harm from LabMD's collection of Personal Information of consumers was not outweighed by harms caused or likely to be caused to, and not reasonably avoidable by, consumers.

508. The Commission's inquisition substantially interfered with LabMD's operations. (Daugherty, Tr. 1028-1034).

Response to Finding No. 508:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. To the extent Respondent is attempting to state a claim that it

suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing.

Courts have concluded that lost business revenue is not a violation of the Fifth Amendment's due process rights. In *Odessky v. FTC*, the court held the alleged potential destruction of plaintiffs' business was only a collateral consequence of government action for which plaintiffs have no protected due process rights. *Odessky v. FTC*, 471 F. Supp. 1267, 1272 (D.D.C. 1979). The court determined: "The Supreme Court has emphasized that loss of employment or other economic injuries that result only indirectly from government actions, including government investigations, do not provide a cause of action under the due process clause of the fifth amendment. *Id.* The Court further stated that "'even if such collateral consequences were to flow from the Commission's investigations, they would not be the result of any affirmative determinations made by the Commission, and they would not affect the legitimacy of the Commission's investigative function.'" *Id.* at 1272 (quoting *Hannah v. Larche*, 363 U.S. 420, 443 (1960)); *see also Jaymar-Ruby, Inc. v. FTC*, 496 F. Supp. 838, 846 (N.D. Ind. 1980) (holding any competitive injury would amount at most to a "collateral consequence" of the Commission's cooperation in the State's investigation for which no Fifth Amendment protection would apply).

Further, loss of business revenue is not a Fourth Amendment seizure that would violate due process. *See Sousley v. Williams*, No. 13–13950, 2014 WL 4059860, at *8-11 (E.D. Mich. Aug. 15, 2014) (finding lost business revenue is not a Fourth Amendment seizure and state defendants are shielded by qualified immunity from liability on plaintiffs' federal claim that there was a decrease in the value of their business because of the government investigation).

In conclusion, conjectural allegations of harm in the form of collateral consequences of authorized investigations, *SEC v. OKC Corp*., 474 F. Supp. 1031 (N.D. Tex. 1979), or a potential business destruction, *Odessky*, 471 F. Supp. at 1272, do not offend due process.

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).

Response to Finding No. 509:

The proposed finding is unsupported and misleading to the extent it suggests that Complaint Counsel issued burdensome and oppressive discovery requests; Complaint Counsel complied with all relevant FTC rules, regulations and discovery orders of this Court and Respondent has cited to no evidence to the contrary

To the extent the proposed finding attempts to state a legal conclusion regarding the First Amendment, it is unsupported and a misstatement of law. (*See* CCRRCL ¶ 161 (addressing claim of reprisal)).

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).

Response to Finding No. 510:

The Court should disregard the proposed finding because it is not supported by the citation to the record. The proposed finding is also misleading because the Commission initiated its investigation by January 2010, long before Mr. Daugherty stated any public criticisms of the

FTC. (Daugherty, Tr. 993).

To the extent the proposed finding attempts to state a legal conclusion regarding the First Amendment, it is unsupported and a misstatement of law. (*See* CCRRCL ¶ 161 (addressing claim of reprisal)).

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)).

Response to Finding No. 511:

The Court should disregard the proposed finding because it is not supported by the citation to the record. To the extent the proposed finding attempts to state a legal conclusion, the proposed finding is a misstatement of the law. "[A]ctual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted unfair . . . acts or practices." Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014) (internal citations and quotations omitted).

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)).

Response to Finding No. 512:

The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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).

Response to Finding No. 513:

The Court should disregard the proposed finding because it is not supported by the citations to the record. To the extent the finding attempts to state a legal conclusion, it is a

misstatement of the law. A party voluntarily changing its conduct is "not a basis for halting a law enforcement action." *In re The Coca-Cola Co.*, 117 F.T.C. 795, 909 (1994). In addition to the possibility of a respondent resuming the illegal practices absent an order, courts recognize that the illegal conduct's effects "may tend to be perpetuated in practice unless affirmative measures are taken to eradicate them." *Rubbermaid, Inc. v. FTC*, 575 F.2d 1169, 1175 (6th Cir. 1978) (affirming cease and desist order even though respondent abandoned challenged practices and did not intend to resume them). Respondent has not met the "formidable burden of showing that it is absolutely clear the allegedly wrongful behavior could not reasonably be expected to recur." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U. S. 167, 190 (2000). Indeed, Complaint Counsel has presented evidence to the contrary.

The weight of the evidence indicates that LabMD continues to place consumers at risk. (CCCL ¶¶ 60-71). LabMD has no intention of dissolving as a Georgia corporation, retains the personal information of over 750,000 consumers, continues to operate a computer network, and intends to employ the same unreasonable policies and procedures to Personal Information in its possession as it employed in the past. (CCCL ¶¶ 60-64). While the specific facts alleged in the complaint may not recur, this does not mean LabMD "may not return to the general course of conduct with which it is charged," that is, failing to provide reasonable security for consumers' Personal Information. *Int'l Harvester Co.*, Docket No. 9147, 104 F.T.C. 949, 1984 WL 565290, at *92 (1984), For example, LabMD continues to operate a computer network consisting of switches, routers, servers, workstation computers, printers, a scanner, and an Internet connection at Mr. Daugherty's residence, as well as a workstation at a condominium that can remotely connect to a server at the private residence network and a printer for the condominium workstation. (CCFF ¶¶ 251-260). The company also continues to provide past test results to

healthcare providers and continues to collect on monies owed to it. (CCFF ¶ 63). And, as of February 2014, the paper records kept at Mr. Daugherty's residence were observed located in rooms throughout the house and were not secured in any way. (CX0725-A (Martin, Dep. at 22)). Likewise, the patient specimens in the basement were also not secured in any way. (CX0725-A (Martin, Dep. at 23)). As of approximately February 2014, some of the items were kept in the garage and the garage was not always locked. (CX0713-A (Gardner, Dep. at 45)). When Ms. Parr went to Mr. Daugherty's home to help finish up some network work there, Mr. Daugherty was not there and the garage door was up. (CX0713-A (Gardner, Dep. at 45-46)). Nor is there any reason to believe that LabMD will improve it security of its own volition. When a third party identified security issues on LabMD's servers and provided solutions, LabMD failed to remediate the problems over several months. (CCFF ¶¶ 759-771 (Anonymous FTP Writeable root directory vulnerability found on Mapper server in May 2010 penetration test still present during July 2010 penetration test), 781-788 (Anonymous FTP Enabled vulnerability found on Mapper server in May 2010 penetration test still present during July 2010 penetration test), 792-797 (FTP Supports Clear Text Authentication vulnerability found on Mapper server in May 2010 penetration test still present during July 2010 and September 2010 penetration tests), 800-808 (Port 3306 on Mapper server found open and providing access to Microsoft MySQL database program in May 2010 penetration test still present during July penetration test)).

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)).

Response to Finding No. 514:

The Court should disregard the proposed finding because it is unsupported by the citation to the record. In addition, the Court should disregard the proposed finding because it relates to

the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1).

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.").

Response to Finding No. 515:

The proposed finding is irrelevant to LabMD's unfair conduct that is the subject of this lawsuit and the claims, defenses, or proposed relief before this Court. The Court should disregard the proposed finding because it relates to the Commission's pre-complaint investigation and decision to file a complaint in this matter, which are not relevant to the claims, defenses, or proposed relief before this Court. (CCRRFF ¶ 1). Complaint Counsel does not dispute that LabMD provided notice to the individuals in the Day Sheets and copied checks in the Sacramento incident.

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....").

Response to Finding No. 516:

The proposed finding is irrelevant. To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508).

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.").

Response to Finding No. 517:

The proposed finding is irrelevant. (CCRRFF ¶ 508 (claim of business loss is legally unavailing)). The Court should also disregard the proposed finding because it is contradicted by the evidence in the record. Mr. Daugherty, LabMD's principal, testified that restructuring under the Affordable Care Act ("Obamacare") required LabMD's customers to send their specimens elsewhere (CX0709 (Daugherty, Dep. at 130-31); Daugherty, Tr. 1040-41), and that LabMD's future "[d]epends on ObamaCare." (CX0709 (Daugherty, Dep. at 60); Daugherty, Tr. 1040-41). Mr. Daugherty similarly conceded at the preliminary injunction hearing in LabMD's lawsuit against the FTC that the implementation of the Affordable Care Act negatively impacted LabMD's operations and LabMD's future "depend[ed] on Obamacare." *See LabMD, Inc. v. FTC*, Case No. 14-0810, 2014 WL1908716, at *6 n.8 (N.D. Ga. May 12, 2014), *aff'd*, 776 F.3d 1275 (11th Cir. 2015) ("LabMD's claim that the FTC investigation had a crippling effect on its business is questionable in light of Mr. Daugherty's testimony at the Preliminary Injunction hearing . . . At the Preliminary Injunction hearing, Mr. Daugherty conceded that the implementation of the Affordable Care Act, and its resulting effect on cost containment and

market consolidation negatively impacted LabMD's operations, and 'creat[ed] huge anxiety, destruction, consolidation in our customer base.' Mr. Daugherty also conceded that LabMD's future 'depend[ed] on Obamacare, and other than that I don't know.'") (internal citations omitted). Respondent introduced no evidence that any clients left LabMD on the basis of LabMD's or other persons' receipt of service of subpoenas. The only evidence in the record from LabMD's former clients indicates that the proposed finding is false. Former LabMD client SUN stated that it switched to a local laboratory that offered in-house pathology. (CX0726 (Maxey, SUN Designee, Dep. at 47-48)). Former LabMD client Midtown Urology left LabMD only when LabMD informed it that it would no longer be accepting new specimens. (CX0728 (Randolph, Midtown Designee, at 79-81)).

To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508).

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)).

Response to Finding No. 518:

The Court should disregard the proposed finding because it attempts to state a legal conclusion, not a fact. In addition, Complaint Counsel's post-trial brief and proposed findings of fact do not cite to Robert Boback's testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback's testimony.

Moreover, the proposed finding is not supported by the citations to the record and completely without foundation. At his November 2013 deposition, Complaint Counsel asked Mr. Boback a number of questions about the IP address that appears on CX0307:

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

(CX0703 (Boback , Tiversa Designee, Dep. at 97-164)). Mr. Boback's explanation – that one exhibit reflected "an initial disclosure source," while the other reflected a "download" location – was unremarkable, and did not need further inquiry. In any event, during Respondent's examination, Respondent did not ask Mr. Boback a single question regarding CX0307, which Complaint Counsel produced with its Initial Disclosures nearly two months before the November 21, 2013 deposition. Based on the record at that point, Complaint Counsel had no basis to question to question Mr. Boback's testimony.

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 . . .")).

Response to Finding No. 519:

To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508). Otherwise, Complaint Counsel has no specific response.

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).

Response to Finding No. 520:

To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508).

Furthermore, Mr. Daugherty testified that LabMD was in breach of contract with his landlord, as LabMD failed to pay rent while LabMD occupied the Powers Ferry Road location. Mr. Daugherty testified that LabMD last paid rent at its Powers Ferry Road location in October 2013, "and then we were late, and then we haven't paid since. . . ." (CX0709 (Daugherty, Dep. at 140-41)). LabMD did not move out of the Powers Ferry Road location until approximately January 2014. (CCFF ¶¶ 66, 69).

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.").

Response to Finding No. 521:

To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508). Otherwise, Complaint Counsel has no specific response.

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. . . .").

Response to Finding No. 522:

To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508). Otherwise, Complaint Counsel has no specific response.

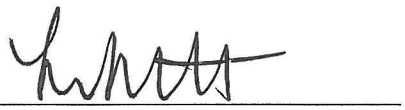
523. In its letter dated January 6, 2014, LabMD stated that the reason for its actions in shutting down its facility was "the conduct of the [FTC]" in that the FTC's actions "subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data–security vulnerability." (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.").

Response to Finding No. 523:

The Court should disregard the proposed finding because it merely provides an opinion and does not state any fact. To the extent Respondent is attempting to state a claim that it suffered a business loss for which it is entitled to damages or which invalidates this proceeding, it is legally unavailing. (CCRRFF ¶ 508).

Dated: September 4, 2015

Respectfully submitted,



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

Complaint Counsel

CERTIFICATE OF SERVICE

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

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

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

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

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

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

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

CERTIFICATE FOR ELECTRONIC FILING

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

September 4, 2015

By: _____

Jarad Brown
Federal Trade Commission
Bureau of Consumer Protection