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

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

<u>RESPONDENT LABMD, INC.'S REPLY TO COMPLAINT COUNSEL'S PROPOSED FINDING OF FACTS</u>

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

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

DATED: SEPTEMBER 3, 2015

COUNSEL FOR RESPONDENT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. LabMD, located in Atlanta, Georgia, is a company that offers medical laboratory services to doctors' offices in at least seven states. From January 1, 2005 through February 10, 2014, its revenue totaled approximately $35-40 million. LabMD is not currently accepting new medical specimens for testing.

Response to Finding No. 1

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record").

2. LabMD collected and maintains Personal Information of consumers, including name, phone number, address, date of birth, Social Security number, payment card and checking account information, health insurance information, diagnoses, and laboratory test results. It collected the information from its physician-clients as well as directly from consumers in connection with payment in some cases. LabMD maintains the Personal Information of at least 750,000 consumers; it provided no services to at least 100,000 of those consumers.

Response to Finding No. 2

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record").

3. LabMD operates a computer network. In addition to supplying computer equipment to some of its physician-clients so they could submit consumer Personal Information to it, LabMD also operates an internal computer network. Previously, the network consisted of employee computers, servers, and hardware, and was used to, among other things, receive orders for tests from its physician-clients, report test results, seek reimbursement from insurance companies, prepare bills, prepare medical records, and process payments. Currently, LabMD's network, including servers containing

Personal Information, is set up at the residence of Michael Daugherty, LabMD's President and CEO, and a corporate condominium. The network is connected to the Internet, and a workstation at the condominium can connect to the servers located in the residence.

Response to Finding No. 3

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record").

4. LabMD failed to provide reasonable security for the Personal Information it collected and maintains. Its failures were multiple, and are likely to cause substantial consumer injury.

   a. LabMD did not have a comprehensive information security program. Prior to 2010, the only written document provided to employees was an employee manual, which contained cursory information on a few aspects of data security but was not comprehensive. In 2010, LabMD created information security documents. Some of the policies memorialized in 2010 were not enforced in 2008 and 2009 when they were allegedly in force, and were not fully enforced after being written in 2010. Furthermore, the 2010 policies are not comprehensive and do not provide for reasonable data security.

   b. LabMD did not use reasonable, readily available measures to identify commonly known and reasonably foreseeable risks to the Personal Information in its possession. LabMD did not adequately deploy antivirus solutions, often failing to run scans, update virus definitions, or review the results of antivirus scans. Likewise, LabMD did not adequately deploy firewalls, or review its logs to detect intrusions or vulnerabilities. Furthermore, although LabMD conducted manual inspections of workstations and servers, these inspections were not performed systematically or proactively. In any event, manual inspections are not an adequate substitute for automated tools, such as the tools described below. LabMD did not use automated risk assessment tools, such as penetration testing, intrusion detection systems, intrusion protection systems, or file integrity monitors. It did not obtain penetration testing of its network until 2010; the standard industry-practice testing that was finally performed revealed numerous "critical" and "urgent" vulnerabilities.

c. LabMD did not use adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs. Nothing prevented staff from accessing patient information that they did not need, and LabMD cannot specify what information staff members had access to. Sales representatives were also able to access patient data. Furthermore, LabMD collected more information than it needed, and never deleted any Personal Information even after it was no longer needed.

d. LabMD did not adequately train employees to safeguard Personal Information. LabMD did not provide training to its IT employees regarding data security, nor to its non-IT employees on how to safeguard patient data. LabMD also did not provide written materials regarding data security to its employees until 2010, and it did not provide training on those materials.

e. LabMD did not require employees to use common authentication-related security measures. It did not implement policies prohibiting employees from using weak passwords, did not require that passwords be changed, and did not prevent the sharing of access credentials. LabMD also did not implement strong password policies for its network infrastructure. Physician-clients were permitted to use weak passwords on the computers LabMD supplied that were used to transmit Personal Information to LabMD.

f. LabMD did not maintain and update operating systems and other devices. Servers used an operating system for two years after the vendor stopped supporting the system, myriad unpatched vulnerabilities on its servers placed Personal Information at risk of compromise, and LabMD used insecure applications for years after updates were recommended.

g. LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal information. LabMD employees were given administrative access to workstation computers, which allowed them to install software on the computers, including software downloaded from the Internet. LabMD stored backups of Personal Information on an employee workstation computer. Finally, LabMD failed to reasonably deploy and configure firewalls by, for example, failing to close unneeded ports and implement software firewalls on employee workstation computers.

Response to Finding No. 4

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”).

5. LabMD did not discover, detect, or correct its security failures, despite the availability of free and low-cost solutions in many instances.

Response to Finding No. 5

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that “[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”).

6. LabMD’s data security practices pose a likelihood of substantial of harm to the consumers whose Personal Information it maintains. This harm is not reasonably avoidable by consumers themselves; many did not know their specimens were sent to LabMD for analysis, and could not discover LabMD’s data security practices. The likelihood of harm is illustrated by two security incidents. In the first, a file containing the Personal Information of approximately 9,300 consumers was found on a peer-to-peer file-sharing network. In the second, documents containing the Personal Information of approximately 600 consumers and copies of 10 checks were found concurrent with the arrest of two suspects who later pleaded guilty to identity theft.

Response to Finding No. 6

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that “[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”).

7. Consumers whose Personal Information LabMD maintains are likely to suffer identity theft, including new account fraud, existing non-card fraud, existing card fraud, and medical identity theft. These types of fraud and identity theft can lead to substantial harm, not only in the form of monetary loss and loss of time spent remediating issues,

but also as physical harm in the case of medical identity theft as well as reputational and privacy harms from the disclosure of medical conditions.

Response to Finding No. 7

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record").

8. Intentionally left blank.

9. Intentionally left blank.

1. DEFINITIONS

10. **1718 File**: The 1,718-page LabMD Insurance Aging report with the filename "insuranceaging_6.05.071.pdf" that is identified as the "P2P insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint, copies of which are located at CX0008 (*in camera*), CX0009 (*in camera*), CX0010 (*in camera*), CX0011 (*in camera*), and CX0697 (*in camera*), and a redacted copy of which is located at RX072. (JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 1).

Response to Finding No. 10

Respondent has no specific response.

11. **Consumer**: A natural person. The patients of LabMD's physician-clients are consumers as that term is used in Section 5(n) of the Federal Trade Commission Act, 15 U.S.C. § 45(n). (JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 1, 2).

Response to Finding No. 11

Respondent has no specific response.

12. **Personal Information**: Individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or

processor serial number. Protected health information as defined in 45 C.F.R. § 160.103 ("PHI") is Personal Information. (JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 1-2).

Response to Finding No. 12

Respondent has no specific response.

13. **Relevant Time Period**: 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)).

Response to Finding No. 13

Respondent has no specific response.

14. Intentionally left blank.

15. Intentionally left blank.

2. QUALIFICATIONS OF PROPOSED EXPERTS

2.1 Expert on Data Security: Raquel Hill, Ph.D.

16. Dr. Raquel Hill is a tenured professor of Computer Science at Indiana University with over 25 years of experience in computing with expertise in computer security, data privacy, and networking systems. (CX0740 (Hill Report) ¶ 1).

Response to Finding No. 16

Respondent has no specific response.

17. Dr. Hill has a Ph.D. in Computer Science from Harvard University. (CX0740 (Hill Report) ¶ 8). She has designed and taught classes in information and systems security. (CX0740 (Hill Report) ¶ 9).

Response to Finding No. 17

Respondent has no specific response.

18. Dr. Hill has published over 25 peer-reviewed articles and abstracts on various topics, including security for pervasive computing environments, encryption-based access control, smartphone security, and privacy in research datasets. (CX0740 (Hill Report) ¶ 9).

Response to Finding No. 18

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's expert report does not state that she published **peer-reviewed articles** and abstracts on the topics of security for pervasive computing environments, encryption-based access control, smartphone security, and privacy in research datasets. It cannot be established from the citation to the record that Dr. Hill's articles on quality of service in networking, security for pervasive computing environments, encryption-based access control . . . smartphone security, and privacy in research datasets were peer reviewed.

19. Complaint Counsel asked Dr. Hill to assess whether LabMD provided reasonable security for Personal Information within its computer network, and whether any security failures could have been corrected using readily available security measures during the Relevant Time Period. (CX0740 (Hill Report) ¶ 4). Specifically, Dr. Hill was asked to analyze the record evidence relating to the allegations in paragraphs 10 and 11 of the Complaint. (CX0740 (Hill Report) ¶ 45).

Response to Finding No. 19

Respondent has no specific response.

20. For Dr. Hill's rebuttal report, Complaint Counsel asked her to evaluate and opine on LabMD's expert Adam Fisk's expert report, specifically Mr. Fisk's rebuttal to her Initial Expert Report and his opinions regarding LabMD's network security practices. (CX0737 (Hill Rebuttal Report) ¶ 2).

Response to Finding No. 20

Respondent has no specific response.

21. Intentionally left blank.

2.2 Experts on Identity Theft and Medical Identity Theft

2.2.1 James Van Dyke

22. Mr. James Van Dyke is a leader in independent research on customer-related security, fraud, payments, and electronic financial services. He is founder and president of Javelin Strategy & Research (Javelin), which provides strategic insights into customer transactions. He leads the publication of the most rigorous annual, nationally-

representative victim study of identity crimes in the United States. (Van Dyke, Tr. 574-75, 580-81; CX0741 (Van Dyke Report) at 1).

Response to Finding No. 22

Respondent has no specific response.

23. 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. (CX0741 (Van Dyke Report) at 1).

Response to Finding No. 23

Respondent has no specific response.

24. Complaint Counsel asked Mr. Van Dyke to assess the risk of injury to consumers whose personally identifiable information (PII) has been disclosed by LabMD without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure. (Van Dyke, Tr. 598; CX0741 (Van Dyke Report) at 2).

Response to Finding No. 24

Respondent has no specific response.

25. 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. (Van Dyke, Tr. 599-600; CX0741 (Van Dyke Report) at 2, 4).

Response to Finding No. 25

Respondent objects to this proposed finding of fact because Van Dyke did not base his "opinions on the facts of the case." Several assertions that Van Dyke relied on in rendering his opinion were proven to be untrue, specifically:

- Boback's testimony that the file could be found as recently as several weeks prior to November 2013. (Van Dyke, Tr. 604; RX 523 (Van Dyke Dep. at 106-108; CX 0703 (Boback, Dep. at 9)).

- That the 1718 file could be found at four separate locations on the internet. (RX 523 (Van Dyke Dep. at 42; CX 0703 (Boback, Dep. at 52-53)); when the 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

26. Intentionally left blank.

2.2.1.1 Mr. Van Dyke's Methodology

27. 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. The 2014 Identity Fraud report is based on the 2013 Javelin Identity Fraud Survey. (CX0741 (Van Dyke Report) at 4).

Response to Finding No. 27

Respondent objects to this proposed finding of fact because Van Dyke's "analysis of the facts in this case" is based on assertions that have proven to be untrue, specifically:

- Boback's testimony that the file could be found as recently as November 2013. (Van Dyke, Tr. 604; RX 523 (Van Dyke Dep. at 106-108; CX 0703 (Boback, Dep. at 9)).
- That the 1718 file could be found at four separate locations on the internet. (RX 523 (Van Dyke Dep. at 42; CX 0703 (Boback, Dep. at 52-53)); when the 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

Thus, Van Dyke's "analysis of the facts in this case" is flawed because it is based upon erroneous assertions and therefore cannot be the basis for a finding of fact.

28. 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. (Van Dyke, Tr. 601-02).

Response to Finding No. 28

Respondent objects to this proposed finding of fact to the extent that Complaint Counsel contends that Van Dyke's analysis of SSN exposure from LabMD's 1718 File is relevant. In his report, Van Dyke defined unauthorized disclosure of the 1718 File as being found "at four IP addresses." (CX0741(Van Dyke Report) at 8). The 1718 File was not found at any of the four IP addresses contained on CX0019. (Wallace, Tr. 1383). Thus, any of Van Dyke's analysis regarding exposure of information in the 1718 File is irrelevant.

29. Intentionally left blank.

2.2.1.1.1 Javelin 2013 Survey Methodology

30. The 2013 ID Fraud Survey was conducted among 5,634 U.S. adults over age 18. (Van Dyke, Tr. 583; CX0741 (Van Dyke Report) at 4).

Response to Finding No. 30

Respondent has no specific response.

31. This sample is representative of the U.S. census demographics distribution. (Van Dyke, Tr. 580-81, 583; CX0741 (Van Dyke Report) at 4).

Response to Finding No. 31

Respondent has no specific response.

32. Data collection took place from October 9 through 30, 2013. (CX0741 (Van Dyke Report) at 4).

Response to Finding No. 32

Respondent has no specific response.

33. Data is weighted using U.S. Population Benchmarks for adults over age 18 on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current Current Population Survey targets. (Van Dyke, Tr. 580-81, 583; CX0741 (Van Dyke Report) at 4).

Response to Finding No. 33

Respondent has no specific response.

34. Longitudinal comparisons of data from the respective Identity Fraud Surveys were used to identify consumer fraud trends. (Van Dyke, Tr. 583, 585-86; CX0741 (Van Dyke Report) at 4).

Response to Finding No. 34

Respondent has no specific response.

35. Mr. Van Dyke prepared projections that include the number of consumers who will be victims of identity theft or identity fraud, financial impact to consumers, and total resultant losses in reference to the personally identifiable information listed on the

Sacramento Day Sheets whose personally identifiable information LabMD maintains on its computer networks. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 35

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD maintained Day Sheets on its computer networks. Day Sheets were not saved electronically. They were printed and made part of batch reports that were placed in file cabinets with locks on them. (CX 714-A ([Fmr. LabMD Empl.] Dep. at 61-62)). Only the person posting information in the Day Sheet could print it. (CX 714-A ([Fmr. LabMD Empl.] Dep. at 65-66; RX 497 (Gilbreth Dep. at 42-44)).

36. 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 Sheet because those consumers were notified of the unauthorized disclosure of their Personal Information in March 2013. (Van Dyke, Tr. 602-04; CX0741 (Van Dyke Report) at 7).

Response to Finding No. 36

Respondent has no specific response.

37. Intentionally left blank.

2.2.2 Rick Kam, CIPP

38. Mr. Kam is 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. He is president and co-founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. (CX0742 (Kam Report) at 3-5, 25, 29-33).

Response to Finding No. 38

Respondent has no specific response.

39. Complaint Counsel called Mr. Kam as an expert to testify about the risk of consumer injury from medical identity theft and identity theft. (Kam, Tr. 393; CX0742 (Kam Report) at 3, 5).

Response to Finding No. 39

Respondent has no specific response.

40. Complaint Counsel asked Mr. Kam to assess the risk of injury to consumers caused by the unauthorized disclosure of consumers' sensitive Personal Information. (CX0742 (Kam Report) at 5).

Response to Finding No. 40

Respondent has no specific response.

41. Mr. Kam based his opinions of the facts of this case on his experience, a literature review, and documents provided to him by Complaint Counsel. (CX0742 (Kam Report) at 5).

Response to Finding No. 41

Respondent objects to this proposed finding of fact because Mr. Kam did not base his "opinions of the facts of this case." Several assertions that Kam relied on in rendering his opinion were proven to be untrue or not admitted into evidence, specifically:

- The Thompson Reuters CLEAR database, which was not admitted into evidence. (CX0742 (Kam Report) at 7); Chappell, Tr. 371-372)).
- That the 1718 file was found by Tiversa at four separate IP addresses on the internet (CX0742 (Kam Report) at 9,19), when the 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

Thus, Kam's "opinions of the facts of this case" are flawed because they are based upon erroneous information and therefore cannot be the basis for a finding of fact.

42. Intentionally left blank.

2.2.2.1 Mr. Kam's Methodology

43. In analyzing the harm of LabMD's unauthorized disclosures, Mr. Kam considered the nature and extent of the sensitive Personal Information involved in an unauthorized disclosure, including the types of identifiers and the likelihood of re-identification; the unauthorized person who used the protected health information or to whom the disclosure was made; whether the sensitive Personal Information was actually acquired or viewed; and the extent to which the risk to the protected health information has been mitigated. (Kam, Tr. 404-06; CX0742 (Kam Report) at 18).

Response to Finding No. 43

Respondent objects to this proposed finding of fact because Mr. Kam's analysis with regard "to whom the disclosure was made," and whether the "sensitive Personal Information was actually acquired or viewed" is based upon incorrect information directly affecting "to whom the disclosure was made," and whether the "sensitive Personal Information was actually acquired or viewed," specifically:

- That the 1718 file was found by Tiversa at four separate IP addresses on the internet, (RX 523 (Van Dyke Dep. at 42; CX 0703 (Boback, Dep. at 52-53)), when the 1718 File was never found at any of the four IP addresses contained on CX 0019. (Wallace, Tr. 1383).

Thus, Kam's analysis is flawed because it is based upon erroneous facts and therefore cannot be the basis for a finding of fact.

44. Intentionally left blank.

2.3 Rebuttal Expert on Peer-to-Peer Technology: Clay Shields, Ph.D.

45. Dr. Clay Shields is a tenured full Professor in the Computer Science Department of Georgetown University, with expertise in networking and network protocols, computer security, digital forensics, and responding to network and computer system events. (CX0738 (Shields Rebuttal Report) ¶ 1).

Response to Finding No. 45

Respondent has no specific response.

46. Dr. Shields has over 20 years of computer science experience, including in digital forensics research and developing and analyzing network protocols. (CX0738 (Shields Rebuttal Report) ¶ 5).

Response to Finding No. 46

Respondent has no specific response.

47. Dr. Shields research includes work on systems for providing anonymity to users through peer-to-peer technology. (CX0738 (Shields Rebuttal Report) ¶ 7). He was involved in a collaborative effort that resulted in a modified Gnutella client that is widely used by law enforcement to investigate the sharing of child sexual abuse images using the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶ 9).

Response to Finding No. 47

Respondent has no specific response.

48. Dr. Shields was asked to review the report of Adam Fisk and provide opinions about Mr. Fisk's conclusions concerning the LimeWire peer-to-peer file sharing program and the disclosure of the 1718 File. In particular, Dr. Shields was asked to: explain how P2P networks and programs work; provide an opinion responding to Mr. Fisk's discussion of how the 1718 File was made available to the Gnutella p2p network; evaluate Mr. Fisk's opinion regarding the limitations of LimeWire's search functionality; evaluate Mr. Fisk's opinion that "casual LimeWire users" could not find the 1718 File; and evaluate Mr. Fisk's opinion that a thumb drive or email was likely to have been used to transfer the 1718 File to a computer outside LabMD. (CX0738 (Shields Rebuttal Report) ¶ 2).

Response to Finding No. 48

Respondent objects to this proposed finding of fact to the extent it indicates that Mr. Fisk's opinion was that a thumb drive or email was likely to have been used to transfer the 1718 File to a computer outside of LabMD. (CX0738 (Shields Rebuttal Report) ¶ 2). Fisk's report does not say it was "likely," rather he says it was "a possibility," that the 1718 file could have left LabMD on a thumb drive or could have been emailed to a friend. Both methods would have been beyond the data security capabilities and standards for a small company in the 2007-2008 time frame. (RX533 (Fisk Report) at 25).

49. Intentionally left blank.

3. RESPONDENT

3.1 Company Business

50. From at least 2001 through approximately December 2013 or January 2014, Respondent LabMD was in the business of conducting clinical laboratory tests on urological specimen samples from consumers and reporting test results to physicians. (Ans. ¶ 3; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 3, Adm. 7; CX0291 (LabMD Letter to Physicians offices re: Closing) at 1).

Response to Finding No. 50

Respondent has no specific response.

51. Respondent has tested samples from consumers in multiple states, including Alabama, Mississippi, Florida, Georgia, Missouri, Louisiana, Arizona, and Tennessee. (Ans. ¶ 5; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 3, Adm. 7-11; CX0726 (Maxey, SUN Designee, Dep. at 22-24)).

Response to Finding No. 51

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The material cited does not state that the Respondent has tested samples from consumers in Tennessee.

52. The consumers whose samples LabMD tested and from whom LabMD collects payments are located throughout the United States. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 3, Adm. 7-11); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10; CX0726 (Maxey, SUN Designee, Dep. at 17, 21); CX0718 (Hudson, Dep. at 15-17); CX0722 (Knox, Dep. at 19); CX0706 (Brown, Dep. at 16-18); CX0715-A (Gilbreth, Dep. at 50-51); CX0713-A (Gardner, Dep. at 25-26).

Response to Finding No. 52

Respondent has no specific response.

53. Intentionally left blank.

3.2 Corporate Structure

54. LabMD is a Georgia corporation. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 2, Adm. 1).

Response to Finding No. 54

Respondent has no specific response.

55. LabMD is a privately held corporation. (CX0709 (Daugherty, Dep. at 12)).

Response to Finding No. 55

Respondent has no specific response.

56. Michael Daugherty is the sole owner of LabMD. (CX0709 (Daugherty, Dep. at 12)).

Response to Finding No. 56

Respondent has no specific response.

3.3 Revenue and Profitability

57. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35-40 million. (Daugherty, Tr. 1059; CX0709 (Daugherty, Dep. at 127-28)).

<u>Response to Finding No. 57</u>

Respondent has no specific response.

58. LabMD's revenue peaked around 2006 or 2007. (CX0709 (Daugherty, Dep. at 128)).

<u>Response to Finding No. 58</u>

Respondent has no specific response.

59. LabMD's peak annual revenue was approximately $10 million. (CX0709 (Daugherty, Dep. at 128)).

<u>Response to Finding No. 59</u>

Respondent has no specific response.

60. Before 2013, LabMD's approximate annual profit margin was 25%. (Daugherty, Tr. 1058-59)).

<u>Response to Finding No. 60</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Daugherty disputed that LabMD had a profit margin of 25% and instead stated that LabMD had an approximate **blended** profit margin of 25% from 2005-2012. (Daugherty, Tr. 1058-59)).

61. In 2013, LabMD's revenue was approximately $2 million. (CX0709 (Daugherty, Dep. at 128)).

<u>Response to Finding No. 61</u>

Respondent has no specific response.

62. Intentionally left blank.

3.4 Wind-Down and Current Status

63. Starting in approximately December 2013 or January 2014, LabMD stopped accepting specimen samples and conducting tests; it continued to provide past test results to healthcare providers and continues to collect on monies owed to it. (CX0291 (LabMD Letter to Physicians offices re: Closing) at 1; CX0765 (LabMD's

Resps. to Second Set of Discovery) at 6, Resp. to Interrog. 10; CX0710-A (Daugherty, LabMD Designee, Dep. at 195); CX0725-A (Martin, Dep. at 25); CX0713-A (Gardner, Dep. at 37)).

Response to Finding No. 63

Respondent objects to the proposed finding of fact because it is unsupported by the citations to the record. The letter, discovery response, and deposition testimony cited do not contain any statement or indication that LabMD continues to collect on monies owed to it. The only cited material that even relates to collection of monies states that "[b]illing operations will continue **through 2014**." (CX0291 (LabMD Letter to Physicians offices re: Closing) at 1 (emphasis added).

64. LabMD does not intend to dissolve as a Georgia Corporation. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 7, Resp. to Interrog. 11; CX0709 (Daugherty, Dep. at 23)).

Response to Finding No. 64

Respondent has no specific response.

65. Intentionally left blank.

3.5 Location

66. LabMD's principal place of business since approximately January 2014 is Mr. Daugherty's residence and a condominium used as an office located at 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 2-3, Adm. 6; CX0710-A (Daugherty, LabMD Designee, Dep. at 193-94); CX0709 (Daugherty, Dep. at 22-23); (CX0725-A (Martin, Dep. at 11-12); CX0705-A (Bradley, Dep. at 20); CX0713-A (Gardner, Dep. at 43)).

Response to Finding No. 66

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The discovery response and deposition testimony cited do not establish that Mr. Daugherty's residence is a principal place of business for LabMD. The admission cited expressly "denies that LabMD is operated out of two offices" and admits that it operates out of the Parkwood Circle address. (CX0766 (LabMD's Resps. and

Objections to Reqs. for Admission) at 2-3, Adm. 6). Moreover, none of the witnesses testified that Mr. Daugherty's private residence is LabMD's principal place of business. Mr. Daugherty merely testified that the Lytec server and the laboratory information system are stored in his home office, (CX0709 (Daugherty, Dep. at 22-23)); he did not state that his home office is also a principal place of business for LabMD. Mr. Martin's testimony only indicates that LabMD transitioned to two locations, including Mr. Daugherty's residence, and confirms that the information systems and servers are stored there. (CX0725-A (Martin, Dep. at 11-12)).

67. Prior to April 2009, LabMD's principal place of business was 1117 Perimeter Center West, Atlanta, Georgia, 30339 ("Perimeter Center West"). (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 2, Adm. 4).

<u>Response to Finding No. 67</u>

Respondent objects to this finding of fact, and states that LabMD's zip code was 30338. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 2, Adm. 4).

68. LabMD's principal place of business from April 2009 through approximately January 2014 was 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339 ("Powers Ferry Road"). (Ans. ¶ 1; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 2, Adm. 5).

<u>Response to Finding No. 68</u>

Respondent has no specific response.

69. Items were moved from the Powers Ferry Road location to Mr. Daugherty's personal residence. (CX0713-A (Gardner, Dep. at 45)). In February 2014, LabMD's IT personnel, including Jeffrey Martin, Jennifer Parr, and Brandon Bradley, began the process of changing LabMD's computer environment from one location (Powers Ferry Road) to two locations (Mr. Daugherty's residence and the corporate condominium). (CX0725-A (Martin, Dep. at 11-12); CX0705-A (Bradley, Dep. at 20)).

Response to Finding No. 69

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. None of the witnesses testified in the portions of the record cited that LabMD's computer environment changed from one location to two. In the cited testimony, Mr. Martin states that "[c]urrently we are all working on setting up the new environment." When asked what he meant by "new environment," Mr. Martin stated that "LabMD has transitioned from the building that we were in to two locations." He did not testify that they were in the process of changing LabMD's **computer environment** from one location to two locations, as Complaint Counsel suggests. Instead, Mr. Martin testified that the information systems and servers had been moved to Mr. Daugherty's private residence, and a billing workstation had been moved into the corporate condominium. (CX0725-A (Martin, Dep. at 11-12)). The portion of Mr. Bradley's testimony cited by Complaint Counsel merely indicates that Mr. Bradley has worked at both the Powers Ferry Road location and at Mr. Daugherty's residence. Mr. Bradley testified that, once LabMD closed its Powers Ferry Road office, the computer equipment and network from that location was moved to Mr. Daugherty's home office, but this alone does not establish that LabMD's computer environment was moved to two locations in February 2014. (CX0705-A (Bradley, Dep. at 20)).

70. Intentionally left blank.

3.6 LabMD's Collection and Maintenance of Consumers' Personal Information

71. 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; *infra* ¶¶ 72-161).

Response to Finding No. 71

Respondent has no specific response.

72. LabMD does not delete or destroy Personal Information of consumers, but maintains it indefinitely. (CX0710-A (Daugherty, LabMD Designee, Dep. at 60, 215-16, 220-21)).

Response to Finding No. 72

Respondent has no specific response.

73. Personal Information stored on LabMD's network is stored in unencrypted form. (CX0734 (Simmons, IHT at 43); CX0735 (Kaloustian, IHT at 53) (describing Personal Information in Mapper system), 62 (stating that personal information of patients in Mapper system was not encrypted)).

Response to Finding No. 73

Respondent has no specific response.

74. LabMD currently maintains the Personal Information of consumers at 1250 Parkwood Circle, Unit 2201, Atlanta GA 30339, a condominium used as an office (CX0765 (LabMD's Resps. to Second Set of Discovery) at 10-11, Resp. to Interrog. 17), and the personal residence of LabMD's President and Chief Executive officer. (CX0710-A (Daugherty, LabMD Designee, Dep. at 193-94); CX0709 (Daugherty, Dep. at 21-23)).

Response to Finding No. 74

Respondent has no specific response.

75. As of February 2014, hundreds of boxes of LabMD's paper records were kept at Mr. Daugherty's personal residence. (CX0725-A (Martin, Dep. at 13); CX0727-A (Parr, Dep. at 65-66); CX0715-A (Gilbreth, Dep. at 96)).

Response to Finding No. 75

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The deposition testimony cited does not establish that **hundreds of boxes** of LabMD's paper records were kept at Mr. Daugherty's personal residence. The cited deposition testimony of Mr. Martin only establishes the existence—not the amount—of paper records at Mr. Daugherty's personal residence. (CX0725-A (Martin, Dep. at 13)). The testimony of Ms. Parr that Complaint Counsel cites actually refutes this proposed finding of fact, as Ms. Parr testified that she does not know if there are more than 50 boxes of documents stored at Mr. Daugherty's address. When asked "[d]o you know if it's more than 20 [boxes]?" Ms. Parr responded "I don't think so." (CX0727-A (Parr, Dep. at 65-66). Complaint Counsel's citation to Ms. Gilbreth's testimony only establishes that there were "a couple hundred" boxes of day sheets in the storage room of the **Powers Ferry location** when LabMD stopped operating. Mr. Gilbreth's cited testimony does not speak to the records located at Mr. Daugherty's personal residence. (CX0715-A (Gilbreth, Dep. at 96)).

76. Over 50 boxes of patient specimens, including slides and tissue samples, were kept in the basement of Mr. Daugherty's personal residence. (CX0725-A (Martin, Dep. at 14-15); CX0727-A (Parr, Dep. at 68-69); CX0705-A (Bradley, Dep. at 42-43)).

<u>Response to Finding No. 76</u>

Respondent has no specific response.

77. Intentionally left blank.

3.6.1 Amount of Personal Information Collected

78. LabMD maintains the Personal Information of over 750,000 consumers. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 5, Adm. 23).

<u>Response to Finding No. 78</u>

Respondent has no specific response.

79. The data includes the Personal Information of approximately 100,000 consumers for whom LabMD never performed testing. (JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 3; CX0710-A (Daugherty, LabMD Designee, Dep. at 185-90, 192-93, 198); CX0718 (Hudson, Dep. at 23-24, 52-54, 59-62); CX0726 (Maxey, SUN Designee, Dep. at 43-45, 80).

<u>Response to Finding No. 79</u>

Respondent has no specific response.

80. Intentionally left blank.

3.6.2 Collection of Consumers' Personal Information from Physician-Clients

81. Consumers' Personal Information came into the LabMD network from its physician-clients. (CX0725-A (Martin, Dep. at 56); *infra* ¶ 82; §§ 4.6.2.1 (Consumers' Personal Information Transferred to LabMD Electronically) (¶¶ 84-90), 4.6.2.3 (Consumers' Personal Information Transferred to LabMD through LabMD-Supplied Computers) *et seq.* (¶¶ 102-115), 4.6.2.4 (Consumers' Personal Information Transferred to LabMD on Paper) (¶ 117)).

Response to Finding No. 81

Respondent objects to this proposed finding of fact to the extent it cites to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

82. LabMD received consumers' Personal Information from its physician-clients before the physician-clients ordered tests from LabMD. (CX0709 (Daugherty, Dep. at 135-36); Daugherty, Tr. 960-61).

Response to Finding No. 82

Respondent has no specific response.

83. Intentionally left blank.

3.6.2.1 Consumers' Personal Information Transferred to LabMD Electronically

84. LabMD's IT staff set up data transfer of patients' Personal Information from the physician-client's databases to LabMD. (CX0718 (Hudson, Dep. at 36-39)).

Response to Finding No. 84

Respondent has no specific response.

85. In some instances, LabMD imported the Personal Information of all patients of entire physicians' practices for which it provided testing, regardless of whether the patients were to receive testing by LabMD or not. (CX0718 (Hudson, Dep. at 24-25, 52-54,

59-62); Daugherty, Tr. 959-60; CX0730 (Simmons, Dep. at 60-65); CX0725-A (Martin, Dep. at 58-59); CX0717 (Howard, Dep. at 33-38)).

Response to Finding No. 85

Respondent has no specific response.

86. Once LabMD initially imported the Personal Information of the entire patient database of physician-clients, in some instances, the Personal Information of physician-clients' patients was updated to LabMD every three to six hours, to ensure that all new patients' information was imported to LabMD's network, including patients for whom LabMD would not be providing testing. (CX0718 (Hudson, Dep. at 24-25, 52); Daugherty, Tr. 959-61; CX0725-A (Martin, Dep. at 59)).

Response to Finding No. 86

Respondent has no specific response.

87. For some physician-clients from at least January 2012 through February 2014, after an initial transmission to LabMD of all the client's patients' information, additional patients' information was sent to LabMD only when patients had testing performed by LabMD. (CX0725-A (Martin, Dep. at 58-59)).

Response to Finding No. 87

Respondent has no specific response.

88. In yet other instances, physician-clients entered patients' Personal Information, one consumer at a time, and then sent the information to LabMD. (CX0728 (Randolph, Midtown Designee, Dep. at 50-52); CX0725-A (Martin, Dep. at 61-62); CX0726 (Maxey, SUN Designee, Dep. at 39-43)).

Response to Finding No. 88

Respondent has no specific response.

89. The Personal Information physicians transferred to LabMD included names, addresses, dates of birth, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and services, and other information. (CX0735 (Kaloustian, IHT at 53-55); CX0717 (Howard, Dep. at 34-35, 38); CX0718 (Hudson, Dep. at 59-60, 62); CX0726 (Maxey, SUN Designee, at 41-42); CX0728 (Randolph, Midtown Designee, at 48, 50-51)).

Response to Finding No. 89

Respondent has no specific response.

90. Patient Personal Information typically was transmitted to LabMD using a file transfer protocol (FTP), through which information flowed from the doctors' offices to a LabMD server on its network. (CX0711 (Dooley Dep. at 131-32); CX0730 (Simmons, Dep. at 61); CX0710-A (Daugherty, LabMD Designee, at 168); CX0717 (Howard, Dep. at 34-35); CX0724 (Maire, Dep. at 41-43); CX0725-A (Martin, Dep. at 56-60)).

Response to Finding No. 90

Respondent objects to this proposed finding of fact to the extent it omits the word "secure" and thereby suggests that PHI was transmitted to LabMD from doctors' offices using an insecure file transfer protocol (FTP). Information was sent to LabMD from doctor's offices via a secure FTP. (CX 0717 (Howard Dep. at 35, 36, 37, 54); (CX0711 (Dooley Dep. at 132); (Maire, Dep. at 41; (Simmons, Dep. at 61, 128); (Martin, Dep. at 60)). Information came to LabMD from physicians through a secure connection. (CX 0704-A (Boyle, Dep. at 13)).

91. Intentionally left blank.

3.6.2.2 Physician-Clients' Ordering of Tests and Obtaining Results

92. Once the consumers' Personal Information was loaded in LabMD's laboratory application, LabSoft, staff at the physician-client's practice could order tests for the patients through LabSoft using LabMD's online portal by searching for the patient's name, selecting the correct patient from a list of patients in that practice, and entering the current procedural terminology ("CPT") code for testing. (CX0718 (Hudson, Dep. at 24-25); CX0709 (Daugherty, Dep. at 86-87); CX0725-A (Martin, Dep. at 56-57)).

Response to Finding No. 92

Respondent has no specific response.

93. A doctor's office employee could search by name, date of birth, or Social Security number to find a patient's record to order a test. (CX0726 (Maxey, SUN Designee, Dep. at 40, 47, 48)).

Response to Finding No. 93

Respondent has no specific response.

94. Doctors placed test orders for lab tests from LabMD through the Internet using a web interface on the computers LabMD provided. (CX0725-A (Martin, Dep. at 56-57); CX0717 (Howard Dep. at 59)).

Response to Finding No. 94

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD provided all doctors' offices with computers. LabMD provided doctor's offices with computers in some cases. CX0717 (Howard Dep. at 59); CX 0709 (Daugherty Dep. at 83)).

95. When a request for a test was made, a report and labels for the specimen would be printed at the doctor's office. (CX0725-A (Martin, Dep. at 56-57)).

Response to Finding No. 95

Respondent has no specific response.

96. The patient's specimen and the report were then sent to LabMD via FedEx. (CX0725-A (Martin, Dep. at 57)).

Response to Finding No. 96

Respondent has no specific response.

97. Once a LabMD pathologist read the specimen and had a test result, the result was entered into a database. (CX0711 (Dooley Dep. at 132-33); CX0717 (Howard Dep. at 49-50).

Response to Finding No. 97

Respondent has no specific response.

98. The results from the tests LabMD performed could be accessed through a web portal using a user ID and password through LabMD-provided computers or the doctor's offices own computers. (CX0726 (Maxey, SUN Designee, Dep. at 29-31, 48-49); CX0728 (Randolph, Midtown Designee, Dep. at 21-22, 57-58); CX0704-A (Boyle, Dep. at 16, 22, 23); CX0722 (Knox, Dep. at 76-78); CX0717 (Howard, Dep. at 59-60); CX0735 (Kaloustian, IHT at 302-03); Daugherty, Tr. 977).

Response to Finding No. 98

Respondent has no specific response.

99. Doctors were provided with the patient's name, doctor's name and the results when doctors requested the results of the tests LabMD performed. (CX0717 (Howard Dep. at 60)).

Response to Finding No. 99

Respondent has no specific response.

100. The web portal used by LabMD's physician-clients returned test results by accessing Personal Information stored on LabMD's network. (CX0704-A (Boyle, Dep. at 33); CX0711 (Dooley, Dep. at 131-32)).

Response to Finding No. 100

Respondent objects to this proposed finding of fact to the extent that it suggests that LabMD's physician clients had access to Personal information on LabMD's network other than their own patients. The system was set up to limit access of physicians to their patients' information only. (CX 0719 (Hyer, Dep. at 142)). Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The testimony cited lists the type of information included in the test results, but it does not state that accessing this information is **how** the web portal returned test results. Mr. Boyle testified that when doctors uploaded test results from LabMD through the web portal, the client information, patient information, and testing information was included in these reports.

101. Intentionally left blank.

3.6.2.3 Consumers' Personal Information Transferred to LabMD Through LabMD-Supplied Computers

102. LabMD supplied computer equipment to doctor offices, including computers, monitors, bar coder machines, and printers. (CX0730 (Simmons, Dep. at 61-62); CX0726 (Maxey, SUN Designee, Dep. at 23-24, 21, 27-28)); (CX0728 (Randolph, Midtown Designee, Dep. at 27-31, 42); *see also* § 4.7.5 Networked Computers Provided by LabMD to Its Physician-Clients).

Response to Finding No. 102

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD provided all of its physician-clients with computers. LabMD provided doctors' offices with computers in some cases. (CX0717 (Howard Dep. at 59); CX 0709 (Daugherty Dep. at 83)).

103. Consumers' Personal Information was stored on the computers that LabMD supplied to its physician-clients. (CX0730 (Simmons, Dep. at 62); CX0734 (Simmons, IHT at 26)).

Response to Finding No. 103

Respondent has no specific response.

104. Consumers' Personal Information was transferred to LabMD using the computers it supplied to physician-clients. (CX0718 (Hudson, Dep. at 80-81); CX0730 (Simmons, Dep. at 61-62); *see also* §§ 4.6.2.3.1 (Southeast Urology Network, PC), 4.6.2.3.2 (Midtown Urology)).

Response to Finding No. 104

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD provided all of its physician-clients with computers. LabMD provided doctors' offices with computers in some cases. (CX0717 (Howard, Dep. at 59); CX 0709 (Daugherty, Dep. at 83)).

105. The computers were provided to communicate with LabMD's internal network to enable the physician-clients to order pathology testing using the patient Personal Information that had been transferred to LabMD and to receive testing results. (CX0725-A (Martin, Dep. at 57); CX0727-A (Parr, Dep. at 71-72); CX0722 (Knox, Dep. at 69); CX0709 (Daugherty, Dep. at 84)).

Response to Finding No. 105

Respondent objects to this proposed finding of fact to the extent it suggests that Personal Information was transmitted to and from physicians' offices and LabMD through any means other than a secure file transfer protocol (SFTP). (Fisk, Tr. 1169-1170; (CX0717 (Howard, Dep. at 35, 36, 37, 54); (CX0711 (Dooley, Dep. at 132); (Maire, Dep. at 41);

(Simmons, Dep. at 61, 128); (Martin, Dep. at 60)). Information came to LabMD from physicians through a secure connection. (CX 0704-A (Boyle, Dep. at 13)).

106. Intentionally left blank.

3.6.2.3.1 Southeast Urology Network, PC

107. The Southeast Urology Network, PC (SUN) is group of urologists in Tennessee. (CX0726 (Maxey, SUN Designee, Dep. at 17).

Response to Finding No. 107

Respondent has no specific response.

108. SUN was a client of LabMD's from 2003 through May 2012. (CX0726 (Maxey, SUN Designee, Dep. at 22, 83)).

Response to Finding No. 108

Respondent has no specific response.

109. LabMD supplied a computer, monitor, and printer to SUN so that SUN could transfer patient information, including Personal Information, to LabMD. (CX0726 (Maxey, SUN Designee, Dep. at 27-28, 41-42)).

Response to Finding No. 109

Respondent has no specific response.

110. Every hour Personal Information of all consumers on the SUN doctor's office network was sent to LabMD's network through the LabMD-supplied computer. (CX0726 (Maxey, SUN Designee, Dep. at 23-24, 27-28, 43, 45)).

Response to Finding No. 110

Respondent objects to this proposed finding of fact to the extent it suggests that Personal Information was transmitted from SUN to LabMD through any means other than a secure file transfer protocol (SFTP). Information was sent to LabMD from doctor's offices via a secure FTP. (Fisk, Tr. 1169-1170; (CX0717 (Howard, Dep. at 35, 36, 37, 54); (CX0711 (Dooley, Dep. at 132); (Maire, Dep. at 41; (Simmons, Dep. at 61, 128); (Martin, Dep. at

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

111. Intentionally left blank.

3.6.2.3.2 Midtown Urology

112. Midtown Urology was a client of LabMD's from 2001 through January 2014, when LabMD ceased to collect specimens. (CX0728 (Randolph, Midtown Designee, Dep. at 19, 79-81)).

Response to Finding No. 112

Respondent has no specific response.

113. LabMD supplied a computer, monitor, and printer to Midtown so that Midtown could transfer patient information, including Personal Information, to LabMD. (CX0728 (Randolph, Midtown Designee, Dep. at 32-33, 48)).

Response to Finding No. 113

Respondent has no specific response.

114. Midtown Urology has electronic healthcare records for over 50,000 consumers. (CX0728 (Randolph, Midtown Designee, Dep. at 17)).

Response to Finding No. 114

Respondent has no specific response.

115. About 80 to 90 percent of Midtown's patients had tests performed by LabMD, and these patients' Personal Information was provided electronically to LabMD. (CX0728 (Randolph, Midtown Designee, Dep. at 18, 49-51); CX0290 (Midtown Urology Unofficial Protocol of Patient Information Transmittal)).

Response to Finding No. 115

Respondent objects to this proposed finding of fact to the extent it suggests that Personal Information was transmitted to and from physicians' offices and LabMD through any means other than a secure file transfer protocol (SFTP). Information was sent to LabMD from doctor's offices via a secure FTP. (Fisk, Tr. 1169-1170; (CX 0717 (Howard, Dep. at 35, 36, 37, 54); (CX0711 (Dooley, Dep. at 132); (Maire, Dep. at 41; (Simmons, Dep. at

61, 128); (Martin, Dep. at 60)). Information came to LabMD from physicians through a secure connection. (CX 0704-A (Boyle, Dep. at 13)).

116. Intentionally left blank.

3.6.2.4 Consumers' Personal Information Transferred to LabMD on Paper

117. Some doctors' offices would send LabMD Personal Information on paper, including name, date of birth, Social Security number, insurance provider, insurance numbers, addresses, and diagnostic codes, which the LabMD billing department would then process and enter into the laboratory information system SQL database to store the information electronically.

Response to Finding No. 117

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The testimony of Mr. Howard cited by Complaint Counsel does not establish the type of patient information that doctors' offices would send to LabMD on paper. Mr. Howard's cited testimony indicates that some patient information was sent on paper, but it does not denote the type of information as Complaint Counsel suggests. Mr. Howard testified that a patient's "name, date of birth, Social Security number, address[], phone number, insurance information, [and] diagnostic code" would be obtained through the **screen scraper**—not via paper copy. His cited testimony offers no indication that this same information was sent to LabMD in paper format. (CX0717 (Howard, Dep. at 38, 43)).

118. Intentionally left blank.

3.6.2.5 Collection and Maintenance of Consumers' Personal Information In Connection With Filing Insurance Claims

119. LabMD files insurance claims with health insurance companies for charges related to clinical laboratory tests it conducts. (Ans. ¶ 4).

Response to Finding No. 119

Respondent has no specific response.

120. In connection with conducting laboratory tests and filing insurance claims for charges related to the clinical laboratory tests, LabMD was provided with information regarding consumers, including: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers; health care provider names, addresses, and telephone numbers; laboratory tests, test codes, and diagnoses; clinical histories; and health insurance company names and policy numbers. (Ans. ¶ 6; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 5-6, Adms. 21 and 25; CX0765 (LabMD's Resps. to Second Set of Discovery) at 8, Resp. to Interrog. 13).

Response to Finding No. 120

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Neither the Answer nor the discovery responses cited establish that LabMD was provided with the clinical histories of consumers.

121. Intentionally left blank.

3.6.2.5.1 Insurance Aging Reports

122. LabMD's billing department generates insurance aging reports. (CX0706 (Brown, Dep. at 50-51)).

Response to Finding No. 122

Respondent has no specific response.

123. Insurance aging reports showed accounts receivable that had not been paid and were used by billing staff to attempt to collect payments on outstanding claims from patients' insurance companies. (CX0706 (Brown, Dep. at 20); CX0715-A (Gilbreth, Dep. at 15-16); CX0714-A ([Fmr. LabMD Empl.], Dep. at 48-49)).

Response to Finding No. 123

Respondent has no specific response.

124. Insurance aging reports were based on a report from LabMD's Lytec billing system that displayed past-due payments from insurance companies. (CX0706 (Brown, Dep. at 23-24)).

Response to Finding No. 124

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited testimony of Ms. Brown does not establish that the report from the Lytec system displayed past-due payments from insurance companies. (CX0706 (Brown, Dep. at 23-24)).

125. Insurance aging reports are spreadsheets of insurance claims and payments, which may include information such as consumers' names, dates of birth, and SSNs; the American Medical Association CPT codes for the laboratory tests conducted; and health insurance company names, addresses, and policy numbers. (Ans. ¶ 9(a); CX0706 (Brown, Dep. at 54).

Response to Finding No. 125

Respondent has no specific response.

126. Insurance aging reports were saved to the billing manager's workstation. (Daugherty, Tr. 982).

Response to Finding No. 126

Respondent objects to this proposed finding of fact to the extent that it suggests that insurance aging reports were routinely saved to the billing manager's work station as there is evidence in the record to the contrary. Billing manager Brown indicates that there was no need to store any type of aging report. Once they were printed, they were shredded. (CX0706 (Brown, Dep. at 23)). Billing manager Gilbreth testified that electronic records were not kept of the insurance aging reports. (CX0715-A (Gilbreth, Dep. at 53, 38)).

127. Insurance aging reports could be saved as Portable Document Format (PDF) files by some billing employees. (CX0715-A (Gilbreth, Dep. at 36-37)).

Response to Finding No. 127

Respondent objects to this proposed finding of fact because it misstates the evidence in the record as there is evidence in the record to the contrary. Gilbreth actually testifies that she has no knowledge of any type of electronic file to which billing staff could save an insurance aging file. (CX0715-A (Gilbreth, Dep. at 37)).

128. [Former LabMD Employee] received from LabMD's billing manager every month hard copies of insurance aging reports. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 49)). Based on the information in the report, the employee would contact the insurance company, obtain the status of the denied claim, and attempt to find ways for the insurance company to pay the claim. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 49-50)).

Response to Finding No. 128

Respondent has no specific response.

129. Intentionally left blank.

3.6.2.6 Collection of Consumers' Personal Information in Connection With Payments by Consumers

130. Insured patients may pay the part of LabMD's charges not covered by insurance, and uninsured patients may be responsible for the full amount of the charges. (Ans. ¶ 4).

Response to Finding No. 130

Respondent has no specific response.

131. 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).

Response to Finding No. 131

Respondent has no specific response.

132. Patient statements were printed from Lytec and mailed to patients. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 24-27)).

Response to Finding No. 132

Respondent has no specific response.

133. Intentionally left blank.

3.6.2.6.1 Credit Cards

134. Patient statements mailed to consumers had a section for patients to write their credit card number and expiration date. (CX0716 (Harris, Dep. at 19-20)).

Response to Finding No. 134

Respondent has no specific response.

135. When consumers returned completed patient statements with the consumer's credit card information to LabMD, it was provided to the billing department. The billing department ran the credit card number and posted the payment in LabMD's system. (CX0716 (Harris, Dep. at 20-21)).

Response to Finding No. 135

Respondent has no specific response.

136. At LabMD's Perimeter Center West location, the billing department then filed patient statements on which consumers had written their payment card information in an unlocked file cabinet in an unlocked room. (CX0716 (Harris, Dep. at 21-22)).

Response to Finding No. 136

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD's physical security was inadequate. FTC's expert Hill testified that LabMD's policy on physical security was acceptable.

Q. Does that refresh your recollection as to what conclusions you drew concerning LabMD's adherence to the physical principle?

A. Yes

Q. And what conclusion did you draw?

A. I thought that their policy on physical security was acceptable.

(RX524 (Hill Dep. at 119)).

137. After LabMD moved to the Powers Ferry Road location, the billing statements with credit card numbers on them were stored in boxes. The boxes were stored in an open room that was regularly left unlocked. (CX0716 (Harris, Dep. at 28-29)).

Response to Finding No. 137

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD's physical security was inadequate. FTC's expert Hill testified that LabMD's policy on physical security was acceptable.

Q. Does that refresh your recollection as to what conclusions you drew concerning LabMD's adherence to the physical principle?

A. Yes

Q. And what conclusion did you draw?

A. I thought that their policy on physical security was acceptable.

(RX524 (Hill Dep. at 119)).

138. LabMD retained the paper statements for years. (CX0716 (Harris, Dep. at 22-23)). Anyone within the company or anyone walking into the building could have gained access to that room. (CX0716 (Harris, Dep. at 22)).

Response to Finding No. 138

Respondent objects to this proposed finding of fact because it suggests anyone who walked in the building had access to the room where day sheets were stored and ignores testimony in the record that is more descriptive of the actual situation.

Q. Could anyone else at LabMD access these batch reports if they wanted to?

A. If they wanted to if they came into our department. During my time of working there I didn't see anyone who was – like anyone from IT or anyone from Accessioning go to those files. They had no need to.

(CX0714-A ([Fmr. LabMD Empl.], Dep. at 66-67)

139. Intentionally left blank.

3.6.2.6.2 Personal Checks

140. When a patient paid by check or money order and LabMD received that payment by mail, LabMD staff would make a copy of the check or money order. (CX0716 (Harris, Dep. at 23-24, 27); CX0706 (Brown, Dep. at 28-29); CX0715-A (Gilbreth, Dep. at 50-51)).

Response to Finding No. 140

Respondent has no specific response.

141. Personal checks contain a consumer's account number, bank routing number, signature, and often an address and phone number. (CX0088 (*in camera*) (LabMD Copied Checks) at 1-10)).

Response to Finding No. 141

Respondent has no specific response.

142. These checks were scanned and deposited. (CX0713-A (Gardner, Dep. at 25-26)). After the checks were scanned and deposited, they were stored for six months in a drawer in the same room where supplies were kept. (CX0713-A (Gardner, Dep. at 26)). LabMD did not lock the drawer in which the checks were stored. (CX0713-A (Gardner, Dep. at 26-27)).

Response to Finding No. 142

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD's physical security was inadequate. FTC's expert Hill testified that LabMD's policy on physical security was acceptable.

Q. Does that refresh your recollection as to what conclusions you drew concerning LabMD's adherence to the physical principle?

A. Yes

Q. And what conclusion did you draw?

A. I thought that their policy on physical security was acceptable.

(RX524 (Hill Dep. at 119)).

143. 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, 70-71)).

Response to Finding No. 143

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD's physical security was inadequate. FTC's expert, Dr. Hill, testified that LabMD's policy on physical security was acceptable.

Q. Does that refresh your recollection as to what conclusions you drew concerning LabMD's adherence to the physical principle?

A. Yes

Q. And what conclusion did you draw?

A. I thought that their policy on physical security was acceptable.

(RX524 (Hill Dep. at 119)).

144. After LabMD moved from its Perimeter Center West location to its Powers Ferry Road location, the copies of the checks and money orders were stored in boxes. (CX0716 (Harris, Dep. at 28)).

Response to Finding No. 144

Respondent has no specific response.

145. The boxes were stored in an open room that regularly was left unlocked. (CX0716 (Harris, Dep. at 28-29)).

Response to Finding No. 145

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD's physical security was inadequate. FTC's expert Hill testified that LabMD's policy on physical security was acceptable. (RX524 (Hill, Dep. at 119)).

146. LabMD maintains copies of hundreds of personal checks. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 7, Adm. 32).

Response to Finding No. 146

Respondent has no specific response.

147. LabMD has never destroyed any of its copies of checks, and has all the copies of checks it has made since its inception. (CX0733 (Boyle, IHT at 46); CX0716 (Harris, Dep. at 25); *see also* (CX0706 (Brown, Dep. at 31)).

Response to Finding No. 147

Respondent has no specific response.

148. LabMD scanned some of its copied checks to archive them electronically. (CX0733 (Boyle, IHT at 47)).

Response to Finding No. 148

Respondent has no specific response.

149. Intentionally left blank.

3.6.2.6.3 Day Sheets

150. As part of its consumer billing process, LabMD produced reports called Day Sheet transaction detail reports ("Day Sheets"). (CX0715-A (Gilbreth, Dep. at 42)).

Response to Finding No. 150

Respondent has no specific response.

151. Day Sheets are reports that are created, accessed, and printed electronically through LabMD's billing application, Lytec, to ensure payment was received and posted. (CX0733 (Boyle, IHT at 33); CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Fmr. LabMD Empl.], Dep. at 58-59)).

Response to Finding No. 151

Respondent has no specific response.

152. LabMD's billing department uses computers to create Day Sheet spreadsheets of payments received from consumers, which may include Personal Information such as consumers' names; SSNs; and methods, amounts, and dates of payments. (Ans. ¶ 9(b); CX0715-A (Gilbreth, Dep. at 37-38, 46-49)).

Response to Finding No. 152

Respondent has no specific response.

153. Day Sheets could also include billing date; provider number; place of service; diagnosis code, which is a standardized code that identifies the symptoms leading to the procedure being performed; payment code; payment amount; charges; credits; and adjustments. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 63); CX0715-A (Gilbreth, Dep. at 48-49); CX0087 (*in camera*) (LabMD Day Sheets)).

Response to Finding No. 153

Respondent has no specific response.

154. Copies of patient checks were attached to the Day Sheets. (CX0715-A (Gilbreth, Dep. at 50-51)).

Response to Finding No. 154

Respondent has no specific response.

155. Day Sheets could be printed by any of LabMD's billing employees who posted payments or a LabMD billing manager. (CX0715-A (Gilbreth, Dep. at 42); CX0714-A ([Fmr. LabMD Empl.], Dep. at 64-65)). Day Sheets were printed almost every day. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 59)).

Response to Finding No. 155

Respondent has no specific response.

156. Billing employees also had the option of saving Day Sheets electronically to a computer. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 59-60)).

Response to Finding No. 156

Respondent objects to this proposed finding of fact to the extent it indicates that Day Sheets were saved electronically. Former LabMD Employee actually testified that he or she never saved Day Sheets and did not know of anyone who actually saved a Day Sheet. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 60)). FTC is aware that no other LabMD employee testified that Day Sheets could be saved and in fact there is testimony that directly contradicts this proposed finding of fact. Day Sheets were not saved electronically. They were printed and made part of batch reports that were placed in file cabinets with locks on them. (CX 714-A ([Fmr. LabMD Empl.], Dep. at 61-62)). If a batch did not balance then the Day Sheet was shredded and a new one was created. Only balanced Day Sheets were retained. (CX 715-A (Gilbreth, Dep. at 42-44)).

157. Day Sheets were stored in paper files at LabMD. (CX0733 (Boyle, IHT at 33-39); CX0710-A (Daugherty, LabMD Designee, Dep. at 60); CX0715-A (Gilbreth, Dep. at 43-45); CX0714-A ([Fmr. LabMD Empl.], Dep. at 58-61)).

Response to Finding No. 157

Respondent has no specific response.

158. Day Sheet transaction reports were printed in paper format and stored in boxes that were kept in storage rooms, which until approximately 2012 were unlocked. (CX0715-A (Gilbreth, Dep. at 45-46)).

Response to Finding No. 158

Respondent objects to this proposed finding of fact to the extent it indicates that Day Sheets were kept in unlocked storage rooms from LabMD's inception until 2012.

Gilbreth was employed as finance manager, and later became billing manager from August 2007 to December 2013. (CX 715-A (Gilbreth, Dep. at 6, 72). Fmr. LabMD Empl. was employed by LabMD from 2007 through January 2009. (CX 714-A ([Fmr. LabMD Empl.], at 13)). Day Sheets were printed and made part of batch reports that were placed in file cabinets with locks on them. "They weren't locked everyday unless they were done at the end of the day when everyone left, but we all had access to open our filing cabinet and pull a batch to see whatever it is that we needed to see."… (CX 714-A ([Fmr. LabMD Empl.], Dep. at 61-62)). Thus the court cannot find it to be a fact that Day Sheets were kept in unlocked storage rooms until approximately 2012. Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Ms. Gilbreth's cited testimony pertains to the storage of the final Day Sheet transaction reports at LabMD's Powers Ferry location. LabMD did not even move its business operations to the Powers Ferry location until 2009. Moreover, Ms. Gilbreth testified that for the last several years at the Powers Ferry office, the final day sheet transaction report for the current month was kept in an **office** next to hers. She also testified that "[t]he boxed records that were anywhere up to a year and a half or two years were also in that same office. The other boxed records were in two different storage rooms within the building." (CX0715-A (Gilbreth, Dep. at 45-46)).

159. LabMD maintained Day Sheets in filing cabinets, which could be accessed by anyone in the Billing Department or anyone who came into the Billing Department. LabMD maintained no measures to physically stop someone from accessing the Day Sheets. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 66-67)).

Response to Finding No. 159

Respondent objects to this proposed finding of fact because it is not specific to a time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the*

Matter of LabMD, Inc., FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

Respondent further objects to the extent it asks the court to make a finding of fact in the face of contradictory evidence in the record. Day Sheets were printed and made part of batch reports that were placed in file cabinets with locks on them. "They weren't locked everyday unless they were done at the end of the day when everyone left, but we all had access to open our filing cabinet and pull a batch to see whatever it is that we needed to see."… (CX 714-A ([Fmr. LabMD Empl.], Dep. at 61-62)). "If they wanted to if they came into our department. During my time of working there I didn't see anyone who was – like anyone from IT or anyone from Accessioning go to those files. They had no need to." (CX0714-A ([Fmr. LabMD Empl.], Dep. at 66-67)).

160. LabMD had no retention policy for these copies, retained them indefinitely, and has all the Day Sheets it created since it has been in business. (CX0733 (Boyle, IHT at 36-37); CX0710-A (Daugherty, LabMD Designee, Dep. at 60); CX0715-A (Gilbreth, Dep. at 42-44)).

<u>Response to Finding No. 160</u>

Respondent objects to this proposed finding of fact to the extent it states that LabMD had no retention policy when the obvious retention policy was to keep Day Sheets indefinitely.

161. Some of the Day Sheets were scanned and saved to LabMD's computer network as part an archive project by the company. (CX0733 (Boyle, IHT at 37, 46-47)).

<u>Response to Finding No. 161</u>

Respondent has no specific response.

162. Intentionally left blank.

3.7 LabMD's Computer Network

163. LabMD has and uses a computer network in conducting its business. (Ans. ¶ 8).

Response to Finding No. 163

Respondent has no specific response.

164. LabMD's computer network consisted of computers used by employees, servers, hardware needed to allow connections among these devices and the Internet, and software of various types. (CX0711 (Dooley, Dep. at 22-29); CX0202 (Network Diagram – Drawn by Jeremy Dooley at Deposition); CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1-2; CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009); CX0734 (Simmons, IHT at 32-39); CX0735 (Kaloustian, IHT at 48-61); CX0584 (Network Diagram Hand-drawn at Kaloustian IH)). LabMD also supplied computers to physician-clients that were networked to its system. (*Infra* § 4.7.5 (Networked Computers Provided by LabMD to Its Physician-Clients) (¶¶ 263-267)).

Response to Finding No. 164

Respondent objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

165. LabMD's network was similar at its Perimeter Center and Powers Ferry Road locations. (CX0735 (Kaloustian, IHT at 48-50); CX0202 (Network Diagram – Drawn by Jeremy Dooley at Deposition); CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1-2; CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009)).

Response to Finding No. 165

Respondent has no specific response.

166. LabMD uses its computer network to receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to referring physicians' patients; and prepare medical records. (Ans. ¶ 9).

Response to Finding No. 166

Respondent has no specific response.

167. LabMD uses its computer network to access documents related to processing claims and payments. (Ans. ¶ 9).

Response to Finding No. 167

Respondent has no specific response.

168. LabMD used its network to collect consumers' Personal Information from its physician-clients. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 4, Adm. 16-17).

Response to Finding No. 168

Respondent has no specific response.

169. LabMD maintains the Personal Information of more than 750,000 consumers on its network. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 5, Adm. 23).

Response to Finding No. 169

Respondent has no specific response.

170. LabMD maintains specific diagnoses and laboratory results of more than 500,000 different consumers on its network. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 6, Adm. 27).

Response to Finding No. 170

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The request for admission cited by Complaint Counsel actually states "[a]dmit that LabMD [m]aintains on Respondent's Computer Network specific diagnoses and laboratory results [of] about **fewer** than 500,000 different Consumers." (emphasis added). Moreover, Respondent expressly denied this request for admission.

171. Intentionally left blank.

172. Intentionally left blank.

3.7.1 LabMD Internally Managed Its Network

173. From at least 2006, LabMD internally managed its network using in-house IT employees. LabMD did not substantially outsource its network set-up or management. (CX0735 (Kaloustian IHT, at 14-15); CX0719 (Hyer, Dep. at 122); CX0724 (Maire, Dep. at 105)).

Response to Finding No. 173

Respondent objects to this proposed finding of fact due to contradictory testimony in the evidentiary record. Allen Truett started Automated PC Technologies ("APT") in 1996. APT provided technology consulting services to small businesses. (CX0731 (Truett, Dep. at 17-18)). APT began providing services to LabMD around 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX0731 (Truett, Dep. at 25, 72-73)). LabMD IT employee Maire started with LabMD in mid 2007 and left in mid 2008. (CX0724 (Maire, Dep. at 10)). Cypress Communications, Inc. ("Cypress") provided LabMD with Internet and phone services from January 2005 to March or April 2012. (CX0729 (Sandrev, Cypress Designee, Dep. at 18-19, 25-26); CX0719 (Hyer, Dep. at 121); CX0711 (Dooley, Dep. at 26)). At the Powers Ferry Road location as of 2010, LabMD's network consisted of three T-1 Internet lines provided by Cypress coming into the facility and connecting to a router/firewall. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 5, Resp. to Interrog. 6; CX0719 (Hyer, Dep. at 121-22)). Cypress managed LabMD's T-1 lines using a router/firewall, switches, and a monitor provided by Cypress. (CX0719 (Hyer, Dep. at 121-22); CX0443 (LabMD Access Letter Response by Philippa Ellis) at 5, Resp. to Interrog. 6).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The testimony cited by Complaint Counsel does not address when LabMD began using in-house IT employees.

174. Intentionally left blank.

3.7.2 LabMD Used Outside Contractors Only for Limited Tasks

3.7.2.1 Cypress Communications, Inc. Did Not Manage LabMD's Internal Network

175. Cypress Communications, Inc. ("Cypress") provided LabMD with Internet and phone services from January 2005 to March or April 2012. (CX0729 (Sandrev, Cypress Designee, Dep. at 18-19, 25-26); CX0719 (Hyer, Dep. at 121); CX0711 (Dooley, Dep. at 26)).

Response to Finding No. 175

Respondent has no specific response.

176. At the Powers Ferry Road location as of 2010, LabMD's network consisted of three T-1 Internet lines provided by Cypress coming into the facility and connecting to a router/firewall. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 5, Resp. to Interrog. 6; CX0719 (Hyer, Dep. at 121-22)). Cypress managed LabMD's T-1 lines using a router/firewall, switches, and a monitor provided by Cypress. (CX0719 (Hyer, Dep. at 121-22); CX0443 (LabMD Access Letter Response by Philippa Ellis) at 5, Resp. to Interrog. 6).

Response to Finding No. 176

Respondent has no specific response.

177. Cypress provided LabMD's base IP addresses, and the IP addresses assigned to the LabMD servers were static. (CX0719 (Hyer, Dep. at 122)).

Response to Finding No. 177

Respondent has no specific response.

178. Cypress did not manage or secure LabMD's internal network. (CX0729 (Sandrev, Cypress Designee, Dep. at 27); CX0678 (Cypress Communications, Inc. Master Terms and Conditions) at 17; *see also* CX0274 (Responses by Cypress Communications))

Response to Finding No. 178

Respondent has no specific response.

179. Cypress would only test a router it provided to LabMD for risks and vulnerabilities if it received a complaint from LabMD. (CX0729 (Sandrev, Cypress Designee, Dep. at 40)).

Response to Finding No. 179

Respondent has no specific response.

180. Cypress has no record of complaints from LabMD during the relevant time period. (CX0729 (Sandrev, Cypress Designee, Dep. at 41)).

Response to Finding No. 180

Respondent has no specific response.

181. Intentionally left blank.

3.7.2.2 APT Did Not Manage LabMD's Network on an Ongoing Basis

182. Automated PC Technologies ("APT"), run by Allen Truett, provided computer and network service to LabMD through approximately March 2007. (CX0731 (Truett, Dep. at 18, 25, 49-50); *see also* CX0724 (Maire, Dep. at 105) (LabMD did not use outside contractors during Mr. Maire's tenure, beginning mid-2007)).

Response to Finding No. 182

Respondent objects to this proposed finding of fact because it is inaccurate due to contradictory testimony in the evidentiary record. APT began providing services to LabMD around 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX0731 (Truett, Dep. at 25, 72-73)). LabMD IT employee Maire started with LabMD in mid 2007 and left in mid 2008 (CX0724 (Maire, Dep. at 10)).

183. APT did not manage or secure LabMD's internal network. (*Infra* ¶¶ 185-186, 188-189; *see also* CX0737 (Hill Rebuttal Report) ¶ 23).

Response to Finding No. 183

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Complaint Counsel's citation to other proposed findings of fact herein are not citations to the evidentiary record and are therefore prohibited by the Scheduling Order.

Further, the cited portion of Dr. Hill's rebuttal report does not state that APT did not manage or secure LabMD's internal network. Rather, Dr. Hill's rebuttal report addresses the security measures that APT **did deploy**—one or more firewalls and antivirus software. Dr. Hill's statement that APT did not actively monitor the operation of LabMD's firewalls fails to establish that APT did not manage or secure LabMD's internal network in any way.

Moreover, Respondent objects to this proposed finding of fact because it improperly cites to expert testimony to support factual propositions that should be established by fact witnesses or documents. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015); *see also In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

184. APT helped LabMD by installing computer equipment and connecting it to a network. (CX0731 (Truett, Dep. at 25)).

<u>Response to Finding No. 184</u>

Respondent has no specific response.

185. APT monitored LabMD only in response to problems, such as Internet speed and connectivity, raised by LabMD employees. CX0731 (Truett, Dep. at 68-69, 78-79)).

<u>Response to Finding No. 185</u>

Respondent has no specific response.

186. APT did not provide LabMD any information on current network security other than recommendations on purchasing or upgrading firewalls or antivirus software. (CX0731 (Truett, Dep. at 42-43)).

Response to Finding No. 186

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record to the contrary. Truett actually testifies that, as per his contract with LabMD, he implemented network security industry standards and best practices based upon what other medical practices and medical organizations employed. He understood the threats and risk mitigation; and he also understood the precautions to take against them. (CX0731 (Truett, Dep. at 44-46)).

187. CX0035 is an example of a report attached to a monthly invoice sent by APT. (CX0731 (Truett, Dep. at 62); CX0035 (APT Service Invoice)).

Response to Finding No. 187

Respondent has no specific response.

188. Mr. Truett does not recall ever providing any specific evaluation regarding the criticality of potential risks to his clients' networks. (CX0731 (Truett, Dep. at 118-19)).

Response to Finding No. 188

Respondent has no specific response.

189. Mr. Truett does not recall doing any assessment of potential risks and vulnerabilities associated with LabMD's network. (CX0731 (Truett, Dep. at 119)).

Response to Finding No. 189

Respondent objects to this proposed finding of fact to the extent it suggests that no assessment of potential risks and vulnerabilities of LabMD's network was done by APT, when in fact Truett actually testifies that part of the service he provided was to understand threats and assess risks. (CX0731 (Truett, Dep. at 45-46)).

190. 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)).

Response to Finding No. 190

Respondent objects to this proposed finding of fact because it misstates the evidentiary record. Truett actually testified that his agreement with LabMD transitioned from an hourly agreement to a flat-type management-type agreement in 2006. (Truett, Dep. at 28-29)). APT began providing services to LabMD around 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX0731 (Truett Dep. at 25, 72-73)). Thus the court cannot find from this evidence that APT's services were in fact replaced by internal employees.

191. Intentionally left blank.

3.7.3 LabMD's Internal Network Prior to 2014

192. LabMD's internal network prior to 2014 was simple. (CX0740 (Hill Report) ¶ 32). Prior to 2014, LabMD's network consisted of computers used by employees, servers performing various functions, and the hardware needed to allow connections among these devices. (*Infra* §§ 4.7.3.1 (Computers Used by Employees) *et seq.* (¶¶ 194-210), 4.7.3.2 (Servers and Applications) *et seq.* (¶¶ 212-244), 4.7.3.3 (Other Network Hardware) (¶¶ 246-249)). Software was installed on servers and employee computers, and LabMD had Internet access. (*Infra* §§ 4.7.3.1.1 (Operating Systems and Software) (¶¶ 198-199); 4.7.3.2 (Servers and Applications) (¶¶ 214-218); 4.7.3.3 (Other Network Hardware) (¶ 246)).

Response to Finding No. 192

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

193. Intentionally left blank.

3.7.3.1 Computers Used by Employees

3.7.3.1.1 Desktop Computers Used by LabMD Employees at LabMD's Place of Business

194. LabMD's employee desktop computers were on the internal network that was self-managed by LabMD IT staff. (CX0719 (Hyer, Dep. at 122)).

<u>Response to Finding No. 194</u>

Respondent objects to this proposed finding of fact because it is not specific to a time frame as required by the post trial briefing order.

195. Employees in the laboratory and billing departments, and certain other employees, used their LabMD computers to access resources on LabMD's network, including applications that provided access to Personal Information maintained on the network. (CX0734 (Simmons, IHT at 33-35); CX0716 (Harris, Dep. at 72-75); CX0735 (Kaloustian, IHT at 233-34, 240-42); CX0755 (LabMD Response to First Set of Interrogs. and Reqs. for Prod.) at 3, Resp. to Interrog. 1 (LabMD employees could gain knowledge of Personal Information regarding Consumers); CX0760 (LabMD Response to Interrogs. 1 and 2); CX0763 (LabMD Revised Answer to Interrogs. 1 and 2)).

<u>Response to Finding No. 195</u>

Respondent has no specific response.

196. LabMD maintained files containing highly sensitive Personal Information on employee desktop computers, such as the finance/billing manager's computer. (CX0725-A (Martin, Dep. at 174-76); CX0735 (Kaloustian, IHT at 117-20); CX0730 (Simmons, Dep. at 22-26, 38-39); CX0006 (LabMD Policy Manual) at 10 (stating policy of saving copy of Lytec Billing System backup on employee computer); CX0007 (LabMD 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)).

<u>Response to Finding No. 196</u>

Respondent has no specific response.

197. Intentionally left blank.

3.7.3.1.1.1 Operating Systems and Software

198. LabMD installed Windows operating systems on the computers used by its employees. (CX0719 (Hyer, Dep. at 88)).

Response to Finding No. 198

Respondent has no specific response.

199. From December 2008 through April 2010, LabMD IT employees installed antivirus software, LogMeIn software, and a Windows firewall on computers used by LabMD employees. (CX0707 (Bureau, Dep. at 43, 45)).

Response to Finding No. 199

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The citations to the record do not establish that these installations took place from December 2008 through April 2010. The cited testimony of Mr. Bureau addresses the software and firewall installed on computers used by LabMD employees, but it does not speak to the time period during which such installations occurred.

200. Intentionally left blank.

3.7.3.1.2 Laptops Issued to Sales Representatives

201. LabMD provided laptop computers, printers, and cell phones to its sales representatives. (CX0718 (Hudson, Dep. at 179); CX0722 (Knox, Dep. at 51); CX0717 (Howard, Dep. at 62, 90-91)).

Response to Finding No. 201

Respondent has no specific response.

202. Sales representatives could log in with a user ID and password to LabMD's network to see whether a physician-client's requested test was pending or completed. (CX0722 (Knox, Dep. at 56-57)).

Response to Finding No. 202

Respondent has no specific response.

203. Intentionally left blank.

3.7.3.1.3 Remote Access

204. Some LabMD employees could remotely access LabMD's network, including Personal Information maintained on the network. (CX0730 (Simmons, Dep. at 50-53); CX0711 (Dooley, Dep. at 60-61); CX0715-A (Gilbreth, Dep. at 61-63); CX0706 (Brown, Dep. at 7-12)).

Response to Finding No. 204

Respondent has no specific response.

205. Sandra Brown worked from home doing billing work for LabMD using her own computer and a service, LogMeIn.com, which allowed her to access LabMD's system remotely. (CX0706 (Brown, Dep. at 6-7, 10-11)).

Response to Finding No. 205

Respondent has no specific response.

206. LogMeIn is a third-party service that provides remote connections to computers. (CX0725-A (Martin, Dep. at 17); CX0705-A (Bradley, Dep. at 52-53)).

Response to Finding No. 206

Respondent has no specific response.

207. A user of LogMeIn can log in to the service using a user name and password after which a connection was created to the remote computer. (CX0725-A (Martin, Dep. at 17-18); CX0727-A (Parr, Dep. at 40); CX0705-A (Bradley, Dep. at 53-55); CX0715-A (Gilbreth, Dep. at 62)).

Response to Finding No. 207

Respondent has no specific response.

208. LabMD had no security requirements for Ms. Brown's home computer. (CX0706 (Brown, Dep. at 78)).

Response to Finding No. 208

Respondent has no specific response.

209. Users could log into the servers through LogMeIn from any computer. (CX0725-A (Martin, Dep. at 18); CX0705-A (Bradley, Dep. at 60)).

Response to Finding No. 209

Respondent has no specific response.

210. LogMeIn.com allows users to access LabMD's network, including patient billing databases. (CX0706 (Brown, Dep. at 11-12)).

Response to Finding No. 210

Respondent objects to this proposed finding of fact to the extent it suggests that a user could access LabMD's databases simply by logging into LogMeIn. In fact, IT employee Brandon Bradley testified that using LogMeIn, one could access the user screen but still needed to know the passwords to log into the other servers. CX0705-A (Bradley, Dep. at 39)). IT employee Jeff Martin confirms that once a connection is created through LogMeIn users are forced to log in again using a user name and password. (CX0725-A (Martin, Dep. at 18-19)).

211. Intentionally left blank.

3.7.3.2 Servers and Applications

212. LabMD's network included servers that hosted applications, such as billing, laboratory, and email. (CX0711 (Dooley, Dep. at 23-24, 27-28); CX0707 (Bureau, Dep. at 63-64); CX0735 (Kaloustian, IHT at 57-59)).

Response to Finding No. 212

Respondent has no specific response.

213. LabMD's servers also performed webserver, backup, and data mapping functions. (CX0735 (Kaloustian, IHT at 51-54, 59-60)).

Response to Finding No. 213

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

214. LabMD used Windows operating systems for its servers. (CX0719 (Hyer, Dep. at 88)).

Response to Finding No. 214

Respondent has no specific response.

215. From at least November 2004 through at least December 2006, the servers were running a mixture of different server operating systems, including Server 2000 and Server 2003. (CX0711 (Dooley, Dep. at 46)).

Response to Finding No. 215

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Dooley's cited testimony does not establish the time period during which the servers were running a mixture of different server operating systems. Mr. Dooley's testimony only indicates that this might have occurred "[u]ntil [C]urt [Kaloustian] was brought on after Howard left the company . . ."

216. In October 2006, some LabMD servers were running Windows NT 4.0. (CX0735 (Kaloustian, IHT at 18-19, 24-28, 59, 271-74)).

Response to Finding No. 216

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

217. From August 2009 through September 2011, most of the LabMD servers ran Windows 2005 to Windows 2008 operating systems, but there were some older servers that had not been upgraded. (CX0719 (Hyer, Dep. at 88-89)).

Response to Finding No. 217

Respondent has no specific response.

218. LabMD used the default configuration that came preloaded on its servers. (CX0717 (Howard, Dep. at 69)).

Response to Finding No. 218

Respondent has no specific response.

219. Intentionally left blank.

3.7.3.2.1 Mapper Server

220. One of the servers on LabMD's network, called Mapper, processed Personal Information transferred from external sources, primarily LabMD's physician-clients, into data useable by programs and applications LabMD used in its laboratory and billing department. (CX0710-A (Daugherty, LabMD Designee, Dep. at 168); CX0725-A (Martin, Dep. at 82-83); CX0704-A (Boyle, Dep. at 24); CX0711 (Dooley, Dep. at 28-29, 131-33); CX0719 (Hyer, Dep. at 108-09); CX0735 (Kaloustian, IHT at 51-52, 225, 302)).

Response to Finding No. 220

Respondent has no specific response.

221. Once data was processed by the Mapper server, the data was then maintained on servers on the network. (CX0725-A (Martin, Dep. at 82-83); CX0704-A (Boyle, Dep. at 24); CX0711 (Dooley, Dep. at 28-29, 131-33); CX0719 (Hyer, Dep. at 108-09); CX0735 (Kaloustian, IHT at 51-52, 225, 302)).

Response to Finding No. 221

Respondent has no specific response.

222. LabMD's network included the Mapper server at its pre-2009 Perimeter Center West location and at its subsequent Powers Ferry Road location. (CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1-2).

Response to Finding No. 222

Respondent has no specific response.

223. The Mapper server's IP address was 64.190.124.7. (CX0710-A (Daugherty, LabMD Designee, Dep. at 166); CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4).

Response to Finding No. 223

Respondent has no specific response.

224. Intentionally left blank.

3.7.3.2.2 LabNet Server

225. The data from the Mapper is imported into the LabNet server, which hosts LabMD's Laboratory Information System ("LIS" or Laboratory Information Management System "LIMS"). (CX0709 (Daugherty, Dep. at 101); CX0725-A (Martin, Dep. at 82-83, 174); CX0705-A (Bradley, Dep. at 54); *see* CX0735 (Kaloustian, IHT at 50-51) (using LIMS term)).

Response to Finding No. 225

Respondent has no specific response.

226. LabMD's LIS was LabSoft. (CX0735 (Kaloustian, IHT at 50-51)).

Response to Finding No. 226

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

227. LabMD installed LabSoft around 2005 or 2006 to replace the previous LIS. (CX0709 (Daugherty, Dep. at 123)).

Response to Finding No. 227

Respondent has no specific response.

228. Data from the previous LIS was imported into the LabSoft system. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 228

Respondent has no specific response.

229. LabMD used LabSoft software to record laboratory services ordered and performed. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 229

Respondent has no specific response.

230. The LabSoft software uses LabNet software to allow for internal processing, testing, and results of laboratory services. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 230

Respondent has no specific response.

231. LabMD stores consumers' Personal Information, including specific diagnoses and laboratory results as well as more general Personal Information for consumers for whom LabMD did not perform tests, in the LIS on the LabNet server. (CX0710-A (Daugherty, LabMD Designee, Dep. at 193); CX0765 (LabMD's Resps. to Second Set of Discovery) at 8-9, Resp. to Interrog. 14).

Response to Finding No. 231

Respondent has no specific response.

232. LabSoft uses an SQL server database to store and retrieve consumers' Personal Information. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6; CX0711 (Dooley, Dep. at 136); CX0717 (Howard, Dep. at 48); CX0734 (Simmons, IHT at 128-30)).

Response to Finding No. 232

Respondent has no specific response.

233. The LabNet server's IP address was 64.190.124.2. (CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4).

Response to Finding No. 233

Respondent has no specific response.

234. Intentionally left blank.

3.7.3.2.3 Lytec Server

235. LabMD has used Lytec software to perform billing services since 2006. (CX0733 (Boyle, LabMD Designee, IHT at 40); CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 235

Respondent has no specific response.

236. LabMD imported data into the Lytec billing system from the LabNet Laboratory Information System once testing of a tissue sample was complete and the results were ready to file. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 236

Respondent has no specific response.

237. Lytec had its own server on LabMD's network after LabMD moved to the Powers Ferry Road location. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6; CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 2 ("LYTEC SERVER")).

Response to Finding No. 237

Respondent has no specific response.

238. LabMD stores Personal Information on the Lytec server, such as patient names, diagnoses, and lab results of consumers. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 8-9, Resp. to Interrog. 14; CX0709 (Daugherty, Dep. at 74); CX0714-A ([Fmr. LabMD Empl.], Dep. at 24-25 (patient bills printed from Lytec))).

Response to Finding No. 238

Respondent has no specific response.

239. Lytec was available to the billing department and IT personnel. (Daugherty, Tr. 983).

Response to Finding No. 239

Respondent has no specific response.

240. Using a billing number, LabMD is able to use Lytec to discern the identity of the consumer associated with that billing number. (Daugherty, Tr. 1019).

Response to Finding No. 240

Respondent has no specific response.

241. Intentionally left blank.

3.7.3.2.4 Other Servers

242. LabMD's other servers included a mail server, an HL7 server, and a Demographics server. (*Infra* ¶¶ 243-244).

Response to Finding No. 242

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

243. LabMD's mail function was on the billing server at LabMD's pre-2009 Perimeter Center West location, (CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1 ("Billing/mail SERVER")), and was housed on its own server at the Powers Ferry Road location. (CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 2; CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009)). Its external IP address was 64.190.124.3. (CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4). As of 2010, LabMD stored archive copies of its LabNet data on the HL7 server. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6). HL7 is an abbreviation for Healthcare language 7, which was a standard language in 2004. (CX0717 (Howard, Dep. at 35)).

Response to Finding No. 243

Respondent has no specific response.

244. One of LabMD's servers was called Demographics or Demo. (CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1-2;

CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009); CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4; CX0313 (LabMD IT Project Outline - Network, Hardware, Software changes) at 2). Its external IP address was 64.190.124.8. (CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4).

Response to Finding No. 244

Respondent has no specific response.

245. Intentionally left blank.

3.7.3.3 Other Network Hardware

246. In addition to the workstations and servers, LabMD's network also had switches and routers, which did not have logging capability, to connect its devices together and allow them to connect to the Internet and other outside resources. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 5; CX0717 (Howard, Dep. at 99-100)).

Response to Finding No. 246

Respondent has no specific response.

247. LabMD's network included firewalls. (CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location) at 1-2; CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009)).

Response to Finding No. 247

Respondent has no specific response.

248. LabMD used a ZyWall firewall starting in approximately May 2006. (CX0731 (Truett, Dep. at 60-61); CX0710-A (Daugherty, LabMD Designee, Dep. at 177-78)).

Response to Finding No. 248

Respondent has no specific response.

249. LabMD replaced the ZyWall firewall with a Juniper firewall in 2010. (CX0710-A (Daugherty, LabMD Designee, Dep. at 178); CX0553 (MDS Juniper Proposal); CX0725-A (Martin, Dep. at 16)).

Response to Finding No. 249

Respondent has no specific response.

250. Intentionally left blank.

3.7.4 Internal Network from January 2014 to Present

251. In January 2014, LabMD moved its network from its Powers Ferry Road business premises. (CX0705-A (Bradley, Dep. at 20); CX0725-A (Martin, Dep. at 11-12); CX0727-A (Parr, Dep. at 44-45)).

Response to Finding No. 251

Respondent has no specific response.

252. Part of the network was moved to the private residence of LabMD's owner, Mr. Daugherty. (CX0725-A (Martin, Dep. at 12-13); CX0727-A (Parr, Dep. at 44-46)).

Response to Finding No. 252

Respondent has no specific response.

253. The rest of the equipment was moved to a nearby condominium owned by Mr. Daugherty. (CX0725-A (Martin, Dep. at 11-12, 16-17); CX0727-A (Parr, Dep. at 50); CX0709 (Daugherty, Dep. at 59)).

Response to Finding No. 253

Respondent has no specific response.

254. Located at Mr. Daugherty's residence and networked together are switches, routers, servers, a firewall, workstation computers, printers, a scanner and an Internet connection. (CX0725-A (Martin, Dep. at 12-13, 15-17); CX0705-A (Bradley, Dep. at 22, 28, 29); CX0727-A (Parr, Dep. at 46, 48-49)).

Response to Finding No. 254

Respondent has no specific response.

255. The servers are located in the residence's basement. (CX0725-A (Martin, Dep. at 15-16)). The servers at Mr. Daugherty's residence include the LabNet LIS server, the Lytec billing server, and the e-mail server. (CX0725-A (Martin, Dep. at 19); CX0727-A (Parr, Dep. at 46-47); CX0705-A (Bradley, Dep. at 24); CX0710-A (Daugherty, LabMD Designee, Dep. at 193-94)).

Response to Finding No. 255

Respondent has no specific response.

256. Located at the condominium is a workstation that can remotely connect to the Lytec billing server at the private residence network through the program LogMeIn. (CX0725-A (Martin, Dep. at 17-19); CX0727-A (Parr, Dep. at 49-50)).

Response to Finding No. 256

Respondent has no specific response.

257. Jennifer Parr, Brandon Bradley, Kindell Alvarez, Jeffrey Martin, and Mr. Daugherty all had access to the LIS on the LabNet server during their tenure. (CX0725-A (Martin, Dep. at 21)).

Response to Finding No. 257

Respondent has no specific response.

258. The laboratory information on servers at Mr. Daugherty's residence was accessed when a client requested a historical result report. (CX0725-A (Martin, Dep. at 19)).

Response to Finding No. 258

Respondent has no specific response.

259. In order to obtain a historical result report, the client sends a fax requesting the results and LabMD faxes a result back to the client. (CX0725-A (Martin, Dep. at 20)).

Response to Finding No. 259

Respondent has no specific response.

260. These requests were handled by LabMD employee Kindell Alvarez. (CX0725-A (Martin, Dep. at 20)). She would receive the fax at the condo location, drive the request to Mr. Daugherty's residence, obtain a print out of the results from the server, and then return to the condo location, where she faxed the result to the client. (CX0725-A (Martin, Dep. at 20-21)).

Response to Finding No. 260

Respondent has no specific response.

261. Intentionally left blank.

262. Intentionally left blank.

3.7.5 Networked Computers Provided by LabMD to Its Physician-Clients

263. LabMD provided computer equipment to some of its physician-client's offices, including computers and monitors. (CX0709 (Daugherty, Dep. at 83-84); CX0718 (Hudson, Dep. at 75-77); CX0722 (Knox, Dep. at 64); CX0728 (Randolph, Midtown Urology Designee, Dep. at 21-22, 32-33); CX0726 (Maxey, Southeast Urology Network ("SUN") Designee, Dep. at 26-29); CX0725-A (Martin, Dep. at 56-57); CX0730 (Simmons, Dep. at 61-62); CX0722 (Knox, Dep. at 64)).

Response to Finding No. 263

Respondent has no specific response.

264. The LabMD-provided computers were set up to connect to the Internet. (CX0718 (Hudson, Dep. at 77, 91-92); CX0722 (Knox, Dep. at 66)).

Response to Finding No. 264

Respondent has no specific response.

265. LabMD collected consumer Personal Information through the networked computers it provided to its physician-clients. (*Supra* § 4.6.2.3 (Consumers' Personal Information Transferred to LabMD Through LabMD-Supplied Computers) (¶¶ 102-105)).

Response to Finding No. 265

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

266. LabMD did not have security requirements for the computers it provided to physician-clients. (CX0735 (Kaloustian, IHT at 151-52)).

Response to Finding No. 266

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing

Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

267. LabMD did not collect the LabMD-provided computers at its client SUN's office when SUN stopped using LabMD's services. (CX0726 (Maxey, SUN Designee, Dep. at 86)).

<u>Response to Finding No. 267</u>

Respondent has no specific response.

268. Intentionally left blank.

3.7.5.1 Transfer of Patient Information to LabMD

269. Patient information, including Personal Information, was transmitted to LabMD on the computers supplied by LabMD to its physician-clients. (*Supra* § 4.6.2.3 (Consumers' Personal Information Transferred to LabMD through LabMD-Supplied Computers) (¶¶ 102-105)).

<u>Response to Finding No. 269</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

270. Intentionally left blank.

3.7.5.1.1 Installation and Limited Support of LabMD-Provided Computers in the Offices of Physician-Clients

271. LabMD sales representatives, who did not have any training in data security, ordinarily set up the LabMD-provided hardware in the physician-clients' offices. (CX0718 (Hudson, Dep. at 70-73, 114-15, 137, 139)).

Response to Finding No. 271

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The deposition testimony cited by Complaint Counsel does not establish that LabMD sales representatives ordinarily set up the LabMD-provided hardware in the doctors' offices or that these sales representatives did not have any training in data security.

The testimony of Ms. Hudson cited by Complaint Counsel does not demonstrate that LabMD sales representatives ordinarily set up the LabMD-provided hardware in the physician-clients' offices. Ms. Hudson's testimony only reveals that it was common for her personally to set up the hardware at the doctors' offices. She testified that "I was the person setting up the computers and I was the person in most of my accounts–on occasion there was technical support from home office, but–setting up whatever had to be set up on the computers." This testimony does not suggest that it was common for all LabMD sales representatives to set up the hardware in the doctors' offices.

Moreover, Ms. Hudson's testimony as to whether she received any training in data security is unclear. She testified that "the extent of our information technology training was how to set up hardware and how to establish LogMeIn and probably also how to set up LabSoft on a computer . . ." When asked if it was her testimony that she received no data security training with respect to informational technology during those training sessions, she stated "I would – nothing outside of basically what a sales rep needs to know, which is assurances that we are HIPAA compliant, that we . . . take precautions with clients' data and you should feel comfortable letting them know we will manage their data carefully. I don't think we were trained on how that's done because it wasn't our job." This response does not necessarily establish that Ms. Hudson did not have **any** training in data security. Further, Ms. Hudson was asked about her training **personally**. She did not testify as to any data security training other LabMD sales representatives might have completed.

272. LabMD's IT staff occasionally went to the site of a physician-client's practice to help install equipment. (CX0718 (Hudson, Dep. at 34-35, 206-07); CX0722 (Knox, Dep. at 66)).

Response to Finding No. 272

Respondent has no specific response.

273. Before shipping to physician-clients' offices, LabMD IT personnel would install software, including the LabMD web portal, on computers intended for doctors' offices. (CX0707 (Bureau, Dep. at 43-44)).

Response to Finding No. 273

Respondent has no specific response.

274. Midtown Urology, one of LabMD's physician-clients, relied on LabMD to service and update the computer equipment that LabMD provided. (CX0728 (Randolph, Midtown Designee, Dep. at 64-65)).

Response to Finding No. 274

Respondent has no specific response.

275. Intentionally left blank.

3.7.5.1.2 Access to Computers and Lack of Restrictions on Use of LabMD-Provided Computers in Physician-Clients' Offices

276. LabMD did not control how the computers placed in physician-clients' offices were used. (CX0734 (Simmons, IHT at 25-26)).

Response to Finding No. 276

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Ms. Simmons did not definitively state that LabMD did not control how the computers placed in physician-clients' offices were used. Rather, Ms. Simmons stated that LabMD "had computers in doctors' offices and **couldn't necessarily** control how they were being used." (emphasis added).

277. LabMD's physician-clients could use the LabMD-provided equipment for whatever additional purposes they chose; the equipment was not locked down in any way. (CX0718 (Hudson, Dep. at 77)).

Response to Finding No. 277

Respondent has no specific response.

278. Sales representatives did not communicate any restrictions on the use of LabMD-provided equipment to physician-clients. (CX0718 (Hudson, Dep. at 92-93)).

Response to Finding No. 278

Respondent has no specific response.

279. Intentionally left blank.

3.8 Relevant LabMD Employees and Contractors

280. In 2007, LabMD had approximately 35-60 employees. (CX0736 (Daugherty IHT at 40-41)). In February 2013, LabMD had approximately 35-40 employees. (CX0736 (Daugherty, IHT at 40)).

Response to Finding No. 280

Respondent has no specific response.

281. Intentionally left blank.

3.8.1 John Boyle

282. John Boyle worked for LabMD from November 1, 2006 until the end of August 2013 as the Vice President of Operations and General Manager. (CX0704-A (Boyle, Dep. at 6-8)).

Response to Finding No. 282

Respondent has no specific response.

283. Mr. Boyle oversaw the laboratory, IT, customer service, and billing departments. (CX0704-A (Boyle, Dep. at 9)).

Response to Finding No. 283

Respondent has no specific response.

284. Intentionally left blank.

3.8.2 Brandon Bradley

285. Brandon Bradley worked for LabMD from May 2010 until February 7, 2014. (CX0705-A (Bradley, Dep. at 7-8)).

Response to Finding No. 285

Respondent has no specific response.

286. Mr. Bradley's duties included setting up desktop computers and installing necessary software. (CX0725-A (Martin, Dep. at 10); CX0705-A (Bradley, Dep. at 8-9)).

Response to Finding No. 286

Respondent has no specific response.

287. Mr. Bradley was responsible for antivirus functioning on employee workstations. (CX0727-A (Parr, Dep. at 88-89)).

Response to Finding No. 287

Respondent has no specific response.

288. Intentionally left blank.

3.8.3 Sandra Brown

289. Sandra Brown worked for LabMD from May 2005 through May 2006 as the billing manager. (CX0706 (Brown, Dep. at 6-7)).

Response to Finding No. 289

Respondent has no specific response.

290. From May 2006 through March 2013, Ms. Brown continued to perform billing work for LabMD working remotely from her home. (CX0706 (Brown, Dep. at 6-7)).

Response to Finding No. 290

Respondent has no specific response.

291. Ms. Brown was supervised by Michael Daugherty. (CX0706 (Brown, Dep. at 7)).

Response to Finding No. 291

Respondent has no specific response.

292. Intentionally left blank.

3.8.4 Matt Bureau

293. Matt Bureau worked for LabMD from December 2008 through April 2010. (CX0707 (Bureau, Dep. at 7)).

Response to Finding No. 293

Respondent has no specific response.

294. Mr. Bureau was responsible for setting up new computers for LabMD's employees and customers. (CX0707 (Bureau, Dep. at 8, 11-12)).

Response to Finding No. 294

Respondent has no specific response.

295. Mr. Bureau was responsible for supporting LabMD's physician-clients, the computers in the doctors' offices, the computers at LabMD, and the salespeople's laptop computers. (CX0707 (Bureau, Dep. at 9-11, 14)).

Response to Finding No. 295

Respondent has no specific response.

296. Mr. Bureau performed maintenance on LabMD employees' computers at LabMD's office and LabMD computers located at the doctors' offices. (CX0707 (Bureau, Dep. at 48-49)).

Response to Finding No. 296

Respondent has no specific response.

297. Intentionally left blank.

3.8.5 Lou Carmichael

298. Lou Carmichael worked as a consultant for LabMD starting in 2001 or 2002 until approximately 2009 or 2010. (CX0708 (Carmichael, Dep. at 19-20)).

Response to Finding No. 298

Respondent has no specific response.

299. Ms. Carmichael was hired to put a Compliance Program in place, to perform training for the Compliance Program, and to produce materials that a compliance officer could use to train additional staff. (CX0708 (Carmichael, Dep. at 19)).

Response to Finding No. 299

Respondent has no specific response.

300. Ms. Carmichael used the office of Inspector General's guidelines for compliance programs to develop LabMD's Compliance Program, and was experienced and qualified at creating compliance programs. (CX0708 (Carmichael, Dep. at 10-12, 15-16, 21)).

Response to Finding No. 300

Respondent has no specific response.

301. Ms. Carmichael subsequently had a retainer relationship whereby LabMD employees could call her with questions, rather than being on a regular salary or hourly commitment. (CX0708 (Carmichael, Dep. at 21-22, 43-44)).

Response to Finding No. 301

Respondent has no specific response.

302. Only salespeople and Michael Daugherty ever called her with questions. (CX0708 (Carmichael, Dep. at 21-22, 65-66)).

Response to Finding No. 302

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Ms. Carmichael did not definitively state that only salespeople and Michael Daugherty called her. Rather, Ms. Carmichael testified that "[she] wouldn't say that really anyone called [her] **very much** except for Mike . . ." (emphasis added). Further, Ms. Carmichael testified that she does not **recall** employees other than Mike Daugherty and salespeople calling her. This testimony does not necessarily establish that these were in fact the only employees who called her.

303. Ms. Carmichael reported to Michael Daugherty. (CX0708 (Carmichael, Dep. at 20)).

<u>Response to Finding No. 303</u>

Respondent has no specific response.

304. Intentionally left blank.

3.8.6 Michael Daugherty

305. Michael Daugherty is the chief executive officer, president, and sole owner of LabMD. (CX0709 (Daugherty, Dep. at 7, 12); CX0736 (Daugherty IHT at 15)).

<u>Response to Finding No. 305</u>

Respondent has no specific response.

306. Mr. Daugherty has been president and CEO since the inception of the company. (CX0736 (Daugherty IHT at 15)).

<u>Response to Finding No. 306</u>

Respondent has no specific response.

307. Mr. Daugherty is the top executive with day to day responsibility for the company. (CX0709 (Daugherty, Dep. at 8-9)).

<u>Response to Finding No. 307</u>

Respondent has no specific response.

308. Other than the physical medical operations of LabMD, Mr. Daugherty has final authority over LabMD's operations. (CX0709 (Daugherty, Dep. at 13-14)).

<u>Response to Finding No. 308</u>

Respondent has no specific response.

309. Mr. Daugherty has a B.A. in economics and psychology from the University of Michigan, Ann Arbor, and does not have any education on information technology ("IT") subjects. (CX0709 (Daugherty, Dep. at 11-12)).

<u>Response to Finding No. 309</u>

Respondent has no specific response.

310. Intentionally left blank.

3.8.7 Jeremy Dooley

311. Jeremy Dooley worked for LabMD from October or November 2004 through December 5, 2006. (CX0711 (Dooley, Dep. at 12-13)).

Response to Finding No. 311

Respondent has no specific response.

312. Mr. Dooley worked on administration of the organization and the software program LabMD used before moving to a website based system, as well as providing technical support to physician-clients. (CX0711 (Dooley, Dep. at 14-17)).

Response to Finding No. 312

Respondent has no specific response.

313. Mr. Dooley was supervised by Michael Daugherty. (CX0711 (Dooley, Dep. at 18)).

Response to Finding No. 313

Respondent has no specific response.

314. Intentionally left blank.

3.8.8 Kim Gardner

315. Kimberly Gardner worked for LabMD from November 2010 to December 27, 2013. (CX0713-A (Gardner, Dep. at 9-10)).

Response to Finding No. 315

Respondent has no specific response.

316. Ms. Gardner was an executive/personal assistant and was the assistant to Mr. Daugherty and Mr. Boyle. (CX0713-A (Gardner, Dep. at 18)).

Response to Finding No. 316

Respondent has no specific response.

317. As part of her job responsibilities, Ms. Gardner handled deposits, which included patient checks and insurance checks. (CX0713-A (Gardner, Dep. at 25)).

Response to Finding No. 317

Respondent has no specific response.

318. Intentionally left blank.

3.8.9 [Former LabMD Employee]

319. [Former LabMD Employee] worked for LabMD from approximately 2007 to 2009 or 2010 as an accounts receivable specialist. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 13, 15)).

<u>Response to Finding No. 319</u>

Respondent has no specific response.

320. [Former LabMD Employee] handled patient payment issues, including processing checks from patients and insurance companies as well as credit card payments. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 15-16)).

<u>Response to Finding No. 320</u>

Respondent has no specific response.

321. [Former LabMD Employee] worked on insurance aging reports; these reports showed accounts receivable that had not been paid. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 48-49)).

<u>Response to Finding No. 321</u>

Respondent has no specific response.

322. Intentionally left blank.

3.8.10 Patricia Gilbreth

323. Patricia Gilbreth worked for LabMD from August 2007 through December 2013 as the finance manager. (CX0715-A (Gilbreth, Dep. at 6)).

<u>Response to Finding No. 323</u>

Respondent has no specific response.

324. In addition to being the finance manager, Ms. Gilbreth was also LabMD's billing manager from mid-2008 through December 2013. (CX0715-A (Gilbreth, Dep. at 7-8)).

<u>Response to Finding No. 324</u>

Respondent has no specific response.

325. As finance manager, Ms. Gilbreth reviewed revenues on a monthly basis and accounts receivable on a daily basis, as well as reviewing the general financial condition of the company. (CX0715-A (Gilbreth, Dep. at 7)).

Response to Finding No. 325

Respondent has no specific response.

326. As billing manager, Ms. Gilbreth supervised the billing employees. (CX0715-A (Gilbreth, Dep. at 12)).

Response to Finding No. 326

Respondent has no specific response.

327. Intentionally left blank.

3.8.11 Nicotra Harris

328. Nicotra Harris worked for LabMD from October 2006 to January 28, 2013 as a billing specialist in LabMD's billing department. (CX0716 (Harris, Dep. at 10-11)).

Response to Finding No. 328

Respondent has no specific response.

329. Ms. Harris was responsible for billing, collections, and posting payments. (CX0716 (Harris, Dep. at 11)).

Response to Finding No. 329

Respondent has no specific response.

330. Ms. Harris prepared patient billing statements for sending to consumers with outstanding balances at LabMD. (CX0716 (Harris, Dep. at 17-18)).

Response to Finding No. 330

Respondent has no specific response.

331. Ms. Harris was supervised by Rosalind Woodson until Ms. Woodson left the company in August 2008. (CX0716 (Harris, Dep. at 13)).

Response to Finding No. 331

Respondent has no specific response.

332. Intentionally left blank.

3.8.12 Patrick Howard

333. Patrick Howard worked for LabMD from March 2004 through March 2007. (CX0717 (Howard, Dep. at 7)).

Response to Finding No. 333

Respondent has no specific response.

334. Mr. Howard was Director of IT. (CX0717 (Howard, Dep. at 8)).

Response to Finding No. 334

Respondent has no specific response.

335. Mr. Howard's position at LabMD focused on running the laboratory IT and specifically the laboratory information system known as LabSoft. (CX0717 (Howard, Dep. at 8, 10)).

Response to Finding No. 335

Respondent has no specific response.

336. Mr. Howard was also responsible for keeping the servers running and for managing network security. (CX0717 (Howard, Dep. at 10)).

Response to Finding No. 336

Respondent has no specific response.

337. Mr. Howard was responsible for patching and updating computers and servers on the LabMD network. (CX0717 (Howard, Dep. at 11)).

Response to Finding No. 337

Respondent has no specific response.

338. Mr. Howard was supervised by Mr. Daugherty. (CX0717 (Howard, Dep. at 8-9)).

Response to Finding No. 338

Respondent has no specific response.

339. Intentionally left blank.

3.8.13 Lawrence Hudson

340. Lawrence Hudson worked for LabMD from approximately January or February 2004 through June or July 2007 as a territory manager. (CX0718 (Hudson, Dep. at 14-15)).

Response to Finding No. 340

Respondent has no specific response.

341. Ms. Hudson’s responsibilities were to acquire business with urology practices as physician-clients, develop marketing materials for sales representatives, take a role in training other sales representatives, and interview new representatives. (CX0718 (Hudson, Dep. at 16-17)).

Response to Finding No. 341

Respondent has no specific response.

342. Ms. Hudson initially reported to Mr. Daugherty, and then to the national sales manager. (CX0718 (Hudson, Dep. at 25-26)).

Response to Finding No. 342

Respondent has no specific response.

343. Intentionally left blank.

3.8.14 Robert Hyer

344. Robert Hyer started his work at LabMD as a two-day consultation on data security in June 2009, which resulted in a two-month contract from approximately July until August 2009. (CX0719 (Hyer, Dep. at 15-16, 30-33)).

Response to Finding No. 344

Respondent has no specific response.

345. Mr. Hyer worked for LabMD full time as Director of IT from approximately August 2009 through approximately September 2011. (CX0719 (Hyer, Dep. at 46-47, 49)).

Response to Finding No. 345

Respondent has no specific response.

346. Mr. Hyer then worked for LabMD as a contractor from approximately September 2011 until approximately March 2012. (CX0719 (Hyer, Dep. at 47)).

Response to Finding No. 346

Respondent has no specific response.

347. Mr. Hyer was in charge of network security. (CX0704-A (Boyle, Dep. at 12)).

Response to Finding No. 347

Respondent has no specific response.

348. Intentionally left blank.

3.8.15 Curt Kaloustian

349. Curt Kaloustian worked for LabMD from October 2006 through April or May 2009. (CX0735 (Kaloustian, IHT at 7, 17)).

Response to Finding No. 349

Respondent has no specific response.

350. Mr. Kaloustian's responsibilities included maintaining the network architecture, maintaining the servers, patches, upgrades, and building the interfaces for client data. (CX0735 (Kaloustian, IHT at 14-15)).

Response to Finding No. 350

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

351. Mr. Kaloustian was responsible for ensuring that data was accurate and correct. (CX0735 (Kaloustian, IHT at 15)).

Response to Finding No. 351

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

352. Mr. Kaloustian initially reported to Mr. Daugherty, and then reported to Mr. Boyle. (CX0735 (Kaloustian, IHT at 16-17)).

Response to Finding No. 352

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

353. Intentionally left blank.

3.8.16 Eric Knox

354. Eric Knox worked for LabMD from February 2005 through May 2007 as a sales representative. (CX0722 (Knox, Dep. at 15-16)).

Response to Finding No. 354

Respondent has no specific response.

355. Mr. Knox initially reported to Mr. Daugherty, and then to a sales manager. (CX0722 (Knox, Dep. at 17)).

Response to Finding No. 355

Respondent has no specific response.

356. Intentionally left blank.

3.8.17 Christopher Maire

357. Christopher Maire worked for LabMD from mid-2007 through June or July 2008 providing tech support. (CX0724 (Maire, Dep. at 10)).

<u>Response to Finding No. 357</u>

Respondent has no specific response.

358. Mr. Maire was the primary IT person who would troubleshoot computers and verify the efficiencies of LabMD's systems. (CX0724 (Maire, Dep. at 44-45)).

<u>Response to Finding No. 358</u>

Respondent has no specific response.

359. Intentionally left blank.

3.8.18 Jeffrey Martin

360. Jeffrey Martin worked for LabMD as IT manager from January 25, 2012 through at least the date of his deposition, February 6, 2014. (CX0725-A (Martin, Dep. at 9)).

<u>Response to Finding No. 360</u>

Respondent has no specific response.

361. Mr. Martin's duties included running queries, creating backups of the laboratory information and billing systems and taking those backups offsite, checking security of the system, and supporting the system to address issues that arose. (CX0725-A (Martin, Dep. at 27, 29)).

<u>Response to Finding No. 361</u>

Respondent has no specific response.

362. Mr. Martin was responsible for network security. (CX0704-A (Boyle, Dep. at 12)).

<u>Response to Finding No. 362</u>

Respondent has no specific response.

363. Mr. Martin was supervised by Mr. Boyle and Mr. Daugherty (CX0725-A (Martin, Dep. at 46)).

<u>Response to Finding No. 363</u>

Respondent has no specific response.

364. Intentionally left blank.

3.8.19 Jennifer Parr

365. Jennifer Parr worked for LabMD from 2010 through February 2014 (CX0727-A (Parr, Dep. at 16-17)).

Response to Finding No. 365

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. This proposed finding of fact suggests that Ms. Parr's employment with LabMD ended in February 2014. However, the testimony cited by Complaint Counsel does not establish that Ms. Parr no longer worked for LabMD after February 2014. Instead, Ms. Parr testified that she stopped working **full-time** for LabMD in February 2014. In fact, at her February 11, 2014 deposition Ms. Parr testified that "[a]s of Friday I worked for LabMD, and **I still do plan to work for LabMD**." (emphasis added) (Parr, Dep. at 16-17)).

366. Ms. Parr was LabMD's Systems Administrator. (CX0727-A (Parr, Dep. at 19)).

Response to Finding No. 366

Respondent has no specific response.

367. Ms. Parr's duties included ensuring: that servers, such as print servers and file servers, functioned properly; that patient data transferred properly from clients; and that the laboratory equipment connected to the network. (CX0727-A (Parr, Dep. at 19-21)).

Response to Finding No. 367

Respondent has no specific response.

368. Ms. Parr was responsible for antivirus functioning on servers. (CX0727-A (Parr, Dep. at 88-89)).

Response to Finding No. 368

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The testimony cited by Complaint Counsel does not indicate that Ms. Parr was responsible for antivirus functioning on servers. Rather, Ms. Parr only testified that she was "the overall Trend Micro person" and that if a virus was found on a server, she would eradicate it.

369. Ms. Parr had no education or training in network security. (CX0727-A (Parr, Dep. at 12)).

Response to Finding No. 369

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Ms. Parr's testimony does not establish that she had no education or training in network security. Rather, Ms. Parr testified that she did not take any courses related to network security during her formal training in information technology. She did not testify that she did not have any training at all in network security.

370. Intentionally left blank.

3.8.20 Alison Simmons

371. Alison Simmons worked for LabMD from October 2006 through August 2009. (CX0730 (Simmons, Dep. at 7)).

Response to Finding No. 371

Respondent has no specific response.

372. Ms. Simmons has a bachelor's degree in computer science. (CX0734 (Simmons, IHT at 17)).

Response to Finding No. 372

Respondent has no specific response.

373. Ms. Simmons was an IT Specialist. (CX0734 (Simmons, IHT at 14)).

Response to Finding No. 373

Respondent has no specific response.

374. Ms. Simmons' responsibilities included responding to phone calls from physician-clients who had problems with LabMD's system, managing and troubleshooting LabMD's database, generating reports, and maintaining computers for the company. (CX0734 (Simmons, IHT at 14-15)).

Response to Finding No. 374

Respondent has no specific response.

375. Intentionally left blank.

3.8.21 Allen Truett

376. Allen Truett's company Automated PC Technologies ("APT") began doing work for LabMD in approximately 2001 or 2002. (CX0731 (Truett, Dep. at 13, 17, 25)).

Response to Finding No. 376

Respondent has no specific response.

377. Mr. Truett does not recall when he stopped working for LabMD, but estimates that it was in 2008 or 2009. (CX0731 (Truett, Dep. at 72-73, 49)).

Response to Finding No. 377

Respondent has no specific response.

378. Intentionally left blank.

3.8.22 Rosalind Woodson

379. Rosalind Woodson worked for LabMD from June 1, 2006 through July 31, 2008. (CX0681 (Rosalind Woodson Dates of Employment) at 7)).

Response to Finding No. 379

Respondent has no specific response.

380. Ms. Woodson was the Billing Manager. (CX0733 (Boyle, IHT at 27)).

Response to Finding No. 380

Respondent has no specific response.

381. Intentionally left blank.

4. LabMD Failed to Provide Reasonable Security for Personal Information on Its Computer Network

382. LabMD engaged in a number of practices that, taken together, failed to provide reasonable security for Personal Information on its computer networks. (Hill, Tr. 95-96, 124, 203; CX0740 (Hill Report) ¶¶ 49, 107; CX0737 (Hill Rebuttal Report) ¶¶ 5, 31; *infra* §§ 5.2 (LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq*. (¶¶ 397-480), 5.3 (LabMD Did Not Use Reasonable, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities) *et seq*. (¶¶ 483-808), 5.4 (LabMD Did Not Use Adequate Measures to Prevent Employees from Accessing Personal Information Not Needed to Perform Their Jobs) *et seq*. (¶¶ 811-849), 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq*. (¶¶ 852-900), 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq*. (¶¶ 903-993), 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043), 5.8 (LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information) *et seq*. (¶¶ 1045-1110)).

Response to Finding No. 382

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

383. Intentionally left blank.

4.1 A Layered Strategy is the Most Effective Way to Provide Reasonable Security

384. Computer threats are evolving. As new measures are put in place to protect against a risk, new risks appear. The result is an ongoing arms race. (Hill, Tr. 109-110; *see also* CX0740 (Hill Report) ¶ 89).

Response to Finding No. 384

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

385. The cycle of implementation and circumvention must be ongoing because intruders frequently discovery ways to evade existing security measures. (Hill, Tr. 109-10; CX0740 (Hill Report) ¶ 89).

Response to Finding No. 385

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Dr. Hill did not testify or state in her expert report that the cycle of implementation and circumvention must be ongoing. The testimony cited by Complaint Counsel only establishes that intruders frequently discover ways to evade existing security measures.

386. A layered data security strategy is the most effective way to provide reasonable security for a network, its computers, and the information it stores. (CX0737 (Hill Rebuttal Report) ¶ 7).

<u>Response to Finding No. 386</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II*, *Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's rebuttal report does not state that a layered data security strategy is most effective. I nstead, Dr. Hill's rebuttal report states that **defense in depth** is the most effective way to provide this security. This distinction is made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

387. A company must take into account the amount and nature of data maintained within its network in determining reasonable and appropriate security measures. (CX0740 (Hill Report) ¶ 49).

<u>Response to Finding No. 387</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II*, *Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

388. A layered approach to security involves a series of coordinated steps: identifying the information and other resources that need to be protected; specifying an appropriate set of security goals and policies for protecting those resources; and

deploying mechanisms that are appropriately configured to enforce those policies. (Hill, Tr. 95-96; CX0740 (Hill Report) ¶¶ 27-31, 52; CX0737 (Hill Rebuttal Report) ¶ 7).

Response to Finding No. 388

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's reports at the cited references does not contemplate a "layered approach," but rather a **defense in depth** approach. This distinction is made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

389. A layered defense may involve implementing security measures at the internet connection layer, the workstation/server layer, and the user account layer. (CX0740 (Hill Report) ¶ 29). Doing so closes the gaps that may be present in any one layer. (CX0740 (Hill Report) ¶ 30).

Response to Finding No. 389

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's reports at the cited references does not contemplate a "layered approach," but rather a **defense in depth** approach. This distinction is made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

390. If there is only one protection mechanism in place, malicious application developers try to determine ways to circumvent that to gain unauthorized access to a system. Reasonable security requires deploying different mechanisms in a layered manner to combat the risks. (Hill, Tr. 199).

<u>Response to Finding No. 390</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

391. A layered approach reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple security measures deployed at different layers of network. (CX0740 (Hill Report) ¶¶ 27-30; CX0737 (Hill Rebuttal Report) ¶¶ 7-8; Hill, Tr. 96-97).

<u>Response to Finding No. 391</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's reports at the cited references does not contemplate a "layered approach," but rather a **defense in depth** approach. This distinction is made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

392. A reasonable data security strategy must take into account not only the size and components of a company's network, but also the volume and sensitivity of the information maintained with the network: the greater the sensitivity and volume of the information, the greater the need for enhanced security measures to provide reasonable security. (CX0740 (Hill Report) ¶¶ 27-30, 75; CX0737 (Hill Rebuttal Report) ¶¶ 7-9; Hill, Tr. 102-03).

<u>Response to Finding No. 392</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

393. 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. (CX0737 (Hill Rebuttal Report) ¶ 9).

<u>Response to Finding No. 393</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

394. When implementing a layered defense strategy, companies should consider certain key principles, including: (1) Don't keep what you don't need; (2) Patch software; (3) Close unused ports; (4) Create and implement security policies; (5) Protect the network with security software; (6) Probe the network with periodic audits, including penetration testing; and (7) Create and implement policies that govern the physical access to devices and data. (Hill, Tr. 104-05; CX0740 (Hill Report) ¶ 31).

Response to Finding No. 394

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's reports at the cited references does not contemplate a "layered approach," but rather a **defense in depth** approach. This distinction is made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

395. LabMD did not reasonably implement these key principles, by: (1) having no policy for deleting patient information by collecting patient information for which it had no business need (*infra* § 5.4.2 (Data Minimization) *et seq.* (¶¶ 830-849); (2) failing to update operating systems and software (*infra* § 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043); (3) failing to close unused ports (*infra* § 5.8.3.2 (LabMD Did Not Properly Configure Its Firewall to Block IP Addresses and Unnecessary Ports) (¶¶ 1094-1105)); (4) failing to have a comprehensive information security program (*infra* § 5.2 LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq.* (¶¶ 397-480; (5) failing to properly deploy firewalls and failing to use intrusion detection or prevention software (*infra* §§ 5.8.3 (LabMD Did Not Reasonably Deploy Firewalls) *et seq.* (¶¶ 1075-1105), 5.3.3 (LabMD Did Not Implement Automated Scanning Tools) *et seq.* (¶¶ 699-712)); (6) failing to conduct penetration testing before May 2010 (*infra* § 5.3.4 (LabMD Did Not Use Penetration Testing Before 2010) (¶¶ 715-7126)); and (7) failing to create and implement policies

to limit access to Personal Information (*infra* §§ 5.4.1 (LabMD Did Not Implement Access Controls) *et seq.* (¶¶ 811-827), 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993)).

<u>Response to Finding No. 395</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

396. Intentionally left blank.

4.2 LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program

397. LabMD did not develop and maintain a comprehensive information security program. (Hill, Tr. 125; CX0740 (Hill Report) ¶ 61; *infra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) *et seq.* (¶¶ 415-443), 5.2.3 (When LabMD Finally Prepared Written Information Security Policies in 2010, They Were Incomplete) *et seq.* (¶¶ 446-455)).

<u>Response to Finding No. 397</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of*

LabMD, Inc., FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

398. A comprehensive written information security program records the organization's current security goals and practices in order to facilitate changes to those goals and practices as security threats continually evolve. ((CX0740 (Hill Report) ¶ 53).

Response to Finding No. 398

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

399. A comprehensive written information security program provides guidance to those who are implementing the plan and those who receive training through the plan. (CX0740 (Hill Report) ¶ 53).

Response to Finding No. 399

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

400. Without a comprehensive written information security program, a company cannot communicate the security goals and practices of the organization to future employees. (CX0740 (Hill Report) ¶ 53).

Response to Finding No. 400

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

401. Because LabMD had no comprehensive program, it deployed technical security measures in an ad hoc manner, leaving it vulnerable to known or reasonably foreseeable threats that could have been mitigated through goal-oriented security measures such as risk assessments, the application of software updates, and employee training. (CX0737 (Hill Rebuttal Report) ¶ 10).

Response to Finding No. 401

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

402. Intentionally left blank.

403. Intentionally left blank.

4.2.1 A Written Comprehensive Information Security Program is a Roadmap for Achieving Reasonable Security

404. A comprehensive information security program is a plan that sets out an organization’s security goals to ensure the confidentiality, integrity, and availability of data and system resources; the written policies that satisfy those goals; and mechanisms that enforce the written policies. (Hill, Tr. 106-07; CX0740 (Hill Report) ¶¶ 52-57; CX0737 (Hill Rebuttal Report) ¶ 7).

Response to Finding No. 404

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

405. Guidelines for securing electronic data in the healthcare context have been available since 1997. (CX0740 (Hill Report) ¶ 60).

Response to Finding No. 405

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

406. Reasonable security balances, on the one side, the severity of a vulnerability or threat and the harm that will result if it is exploited against, on the other side, the cost of measure(s) that remediate the vulnerability or threat. (CX0740 (Hill Report) ¶ 75).

Response to Finding No. 406

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

407. A confidentiality goal/policy ensures that only authorized individuals are able to access data. (CX0740 (Hill Report) ¶ 55).

Response to Finding No. 407

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

408. An integrity goal/policy ensures that data is not inadvertently changed or lost. (CX0740 (Hill Report) ¶ 56).

Response to Finding No. 408

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

409. An availability goal/policy ensures that the computing system and data are accessible, even in the presence of natural disasters or malicious attempts to compromise the system. (CX0740 (Hill Report) ¶ 57).

Response to Finding No. 409

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

410. When an organization fails to develop a comprehensive information security program, it sets itself up to fail at protecting its critical and sensitive resources. (CX0737 (Hill Rebuttal Report) ¶ 7).

Response to Finding No. 410

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

411. A comprehensive information security program should be in writing (1) to provide guidance to those who are implementing the plan and receive training through the plan; (2) to record the organization's current security goals and practices to facilitate changes to those goals and practices as security threats evolve; and (3) to communicate security goals and practices to future employees as turnover occurs. (CX0740 (Hill Report) ¶ 53; Hill, Tr. 107).

Response to Finding No. 411

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

412. LabMD didn't have a roadmap to follow to achieve reasonable security. (CX0737 (Hill Rebuttal Report) ¶ 10).

Response to Finding No. 412

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

413. Intentionally left blank.

414. Intentionally left blank.

4.2.2 Before 2010 LabMD Did Not Have Written Information Security Policies

415. LabMD had no written information security program from 2005 to 2010. (*Infra* ¶ 416-17, § 5.2.2.1 (LabMD's Employee Handbooks, Compliance Policy, and Training Did Not Establish Written Security Policies) *et seq*. (¶¶ 420-443)).

<u>Response to Finding No. 415</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

416. According to LabMD, prior to 2010, some data use policies were included in its Employee Handbook, but other policies were only conveyed verbally. (CX0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions) at 1; CX0445 (LabMD Access Letter Response by Philippa Ellis) at 4).

<u>Response to Finding No. 416</u>

Respondent has no specific response.

417. LabMD's IT employees were not familiar with any written information security policies and procedures during their tenures with the company between 2005 and 2007. (CX0717 (Howard, Dep. at 17); CX0711 (Dooley, Dep. at 35-37)).

<u>Response to Finding No. 417</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The testimony cited only suggests that Mr. Howard and Mr. Dooley were not familiar with any written information security policies. It does not establish that no IT employees were familiar with such policies or, in the alternative, that Mr. Howard and Mr. Dooley were the only IT employees.

418. Intentionally left blank.

419. Intentionally left blank.

4.2.2.1 LabMD's Employee Handbooks, Compliance Policy, and Training Did Not Establish Written Security Policies

420. LabMD maintains that before memorializing its security policies in writing in 2010, LabMD informed employees of its policies through its Employee Handbook, its compliance policy, and its training. (CX0733 (Boyle, LabMD Designee, IHT at 79); CX0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions) at 1).

Response to Finding No. 420

Respondent has no specific response.

421. Intentionally left blank.

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

422. New LabMD employees received an employee handbook. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 88); CX0716 (Harris, Dep. at 48)).

Response to Finding No. 422

Respondent has no specific response.

423. LabMD's Employee Handbook was not a Comprehensive Information Security Program because it did not contain specific policies about protecting data resources and infrastructure. (Hill, Tr. 129; *see also* CX0740 (Hill Report) ¶ 61(a); *infra* § 5.2.3.1 (The Written Policies Prepared by LabMD in 2010 Failed to Address Key Security Policies) (¶¶ 423-455)).

Response to Finding No. 423

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”); *see also* at 3 (stating “[d]o not use ‘*Id.*’ as a cite for proposed findings of fact . . .,” implying that *infra* or *supra* should also not be used.)

424. Apart from the restriction on personal Internet and email usage, LabMD’s Employee Handbook does not contain specific policies about protecting data resources and infrastructure, or explain what, if any, mechanisms LabMD implemented to achieve such goals. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 7; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 7).

Response to Finding No. 424

Respondent has no specific response.

425. LabMD’s Employee Handbook does not include policies for encrypting sensitive information in or attached to emails. (CX0001 (LabMD Employee Handbook Rev. June 2004); CX0002 (LabMD Employee Handbook Rev. Mar. 2008)).

Response to Finding No. 425

Respondent has no specific response.

426. LabMD’s Employee Handbook does not include password policies. (CX0710-A (Daugherty, LabMD Designee, Dep. at 119); CX0001 (LabMD Employee Handbook Rev. June 2004); CX0002 (LabMD Employee Handbook Rev. Mar. 2008)).

Response to Finding No. 426

Respondent has no specific response.

427. Under a section entitled “Privacy of Protected Information,” LabMD’s Employee Handbook states that “LabMD has taken specific measures to ensure [its] compliance with” HIPAA. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6).

Response to Finding No. 427

Respondent has no specific response.

428. HIPAA, and the Security Rule promulgated under it in 2003, 45 C.F.R. Parts 160, 162, and 164, require entities like LabMD to implement reasonable measures to protect the confidentiality, integrity, and availability of sensitive medical information. (CX0405 (HIPAA Security Series 6 – Basics of Risk Analysis and Risk Management (2005)), at 1-2, 14, 16).

Response to Finding No. 428

Respondent objects to this proposed finding of fact because "[t]o be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014).

429. The handbook does not describe any "specific measures" to ensure compliance with HIPAA. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6).

Response to Finding No. 429

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "[t]o be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014))).

430. No "specific measures" that LabMD took to comply with HIPAA were identified to LabMD employees. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 88-89); CX0716 (Harris, Dep. at 51); CX0707 (Bureau, Dep. at 26)).

Response to Finding No. 430

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "To be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014).

431. No LabMD employee — including LabMD's President and CEO — could describe what mechanisms LabMD implemented to achieve the stated goal of "specific measures" to comply with HIPAA. (CX0725-A (Martin, Dep. at 166-67); CX0711 (Dooley, Dep. at 144-46); CX0719 (Hyer, Dep. at 162-63); CX0733 (Boyle, IHT at 248-49); CX0710-A (Daugherty, LabMD Designee, Dep. at 119).

Response to Finding No. 431

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "To be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014)).

Respondent further objects to this proposed finding of fact because it states the goal was specific measures rather than HIPAA compliance. The goal was HIPAA compliance.

> "The Health Insurance Portability and Administrative Act (HIPAA) of 1993 made it illegal for any person in health care to share an individual's protected health care information with anyone other than for specific reasons of treatment, payment or health care operations. Because LabMD has taken specific measures to comply with this law…"

(CX0001 (LabMD Employee Handbook Rev. June 2004) at 6)).

432. Intentionally left blank.

433. Intentionally left blank.

4.2.2.1.2 LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program

434. LabMD's Compliance Program did not include any security policies and procedures. (*Infra* ¶¶ 437-438).

Response to Finding No. 434

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

435. LabMD had a Compliance Program. (CX0708 (Carmichael, Dep. at 19); CX0005 (LabMD Compliance Program effective Jan. 2003)).

<u>Response to Finding No. 435</u>

Respondent has no specific response.

436. LabMD's Compliance Program states that "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 operation uses (an unusual occurrence at LabMD)." (CX0005 (LabMD Compliance Program effective Jan. 2003) at 4).

<u>Response to Finding No. 436</u>

Respondent has no specific response.

437. LabMD's Compliance Program does not itself contain policies and procedures to monitor and insure patient information is secure. (CX0005 (LabMD Compliance Program effective Jan. 2003) at 4; CX0708 (Carmichael, Dep. at 30-31)).

<u>Response to Finding No. 437</u>

Respondent has no specific response.

438. It was not Ms. Carmichael's responsibility as the creator of the Compliance Program to create or include policies and procedures to monitor and ensure patient information is secure. (CX0708 (Carmichael, Dep. at 57-61, 65)).

<u>Response to Finding No. 438</u>

Respondent has no specific response.

439. Intentionally left blank.

440. Intentionally left blank.

4.2.2.1.3 LabMD's Employee Training Was Not a Comprehensive Information Security Program

441. LabMD's non-IT employees did not receive security instruction or training that could address the absence of a written comprehensive information security program. (*Infra* § 5.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information) *et seq*. (¶¶ 867-901)).

Response to Finding No. 441

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

442. LabMD's IT employees did not receive security instruction or training on security. (*Infra* § 5.5.1 (LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information) (¶¶ 858-864)).

Response to Finding No. 442

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

443. LabMD employees consistently testified that they received no instruction or training on security. (*Infra* Section § 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq.* (¶¶ 862-863, 877, 882-885, 888-892, 898-901)).

Response to Finding No. 443

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

444. Intentionally left blank.

445. Intentionally left blank.

4.2.3 When LabMD Finally Prepared Written Information Security Policies in 2010, They Were Incomplete

446. In June 2010, LabMD reduced its purported policies to two written policy manuals, the "LabMD Policy Manual" (CX0006 (LabMD Policy Manual)) and the "LabMD Computer Hardware, Software and Data Usage and Security Policy Manual" (CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual)). (CX0733 (Boyle, IHT at 78-79, 91-92, 97-98); CX0449 (Email D. Rosenfeld to A. Sheer Subject: LabMD Responses to FTC Questions) at 1; CX0445 (LabMD Access Letter Response by Philippa Ellis) at 4; *see* CX0006 (LabMD Policy Manual); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual)).

<u>Response to Finding No. 446</u>

Respondent has no specific response.

447. The policies set forth in LabMD's Policy Manual, CX0006, and LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual, CX0007, were not memorialized in writing as they appear in CX0006 and CX0007 until 2010. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4, Stips. 6-7).

<u>Response to Finding No. 447</u>

Respondent has no specific response.

448. LabMD maintains it created its Policy Manual, CX0006, in 2010 and that CX0006 memorializes in writing the information security practices that LabMD implemented on various dates from 2001 through 2008 and followed in 2007 through 2009. (CX0733 (Boyle, IHT at 78-79, 91-92, 97-98; CX0445 (LabMD Access Letter Response by P. Ellis Jul. 16, 2010) at 4-6; CX0446 (LabMD Access Letter Response by P. Ellis Aug. 30, 2010) at 2).

Response to Finding No. 448

Respondent has no specific response.

449. LabMD maintains that it created its Computer Hardware, Software and Data Usage and Security Policy Manual, CX0007, in 2010 and that CX0007 memorializes in writing LabMD's information security practices as of 2010. (CX0733 (Boyle, IHT at 78-79, 91-92, 97-98)).

Response to Finding No. 449

Respondent has no specific response.

450. Intentionally left blank.

451. Intentionally left blank.

4.2.3.1 The Written Policies Prepared by LabMD in 2010 Failed to Address Key Security Policies

452. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual were missing key elements regarding specific policies on protection of Personal Information in transit, encryption of stored information, and passwords. (CX0740 (Hill Report) ¶ 61(c); Hill, Tr. 131-32; *infra* ¶¶ 453-455).

Response to Finding No. 452

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

453. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual did not include policies that describe how Personal Information is protected during transmission between the physician offices and LabMD. (CX0740 (Hill Report) ¶ 61(c)); CX0006 (LabMD Policy Manual); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual); *supra* § 4.6 (LabMD's Collection and Maintenance of Consumers' Personal Information) *et seq.* (¶¶ 71-115)).

Response to Finding No. 453

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

454. The Policy Manual and the Computer Hardware, Software and Data Usage and Security Policy Manual did not include policies that describe whether sensitive information is to be stored in an encrypted format. (CX0740 (Hill Report) ¶ 61(c); CX0006 (LabMD Policy Manual); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual)).

Response to Finding No. 454

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

455. LabMD's Policy Manual and the Computer Hardware, Software and Data Usage and Security Policy Manual lacked policies about password strength, password re-use, and in the case of CX0006 how often passwords should be changed. (CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24; *infra* § 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq*. (¶¶ 913-914, 920-923, 926-930, 941-942, 946-951, 966, 969-971, 975-983 (password strength), 956-958 (password re-use and change))).

Response to Finding No. 455

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

456. Intentionally left blank.

457. Intentionally left blank.

4.2.4 LabMD Did Not Enforce Some of the Policies in Its Policy Manuals

4.2.4.1 LabMD Did Not Enforce Its Policy to Restrict Downloads from the Internet

458. LabMD's Policy Manual (CX0006) and Computer Hardware, Software and Data Usage and Security Policy Manual (CX0007) include a policy restricting employee downloads by requiring that employees not be given administrative access to their workstation computers. (CX0006 (LabMD Policy Manual) at 21; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 26).

Response to Finding No. 458

Respondent has no specific response.

459. LabMD affirmed that this policy was in effect during the 2007-2008 time frame. (CX0446 (LabMD Access Letter Response by P. Ellis, Aug. 30, 2010) at 2, 6).

Response to Finding No. 459

Respondent has no specific response.

460. Until at least 2009, many LabMD employees had administrative, rather than limited, rights to their computers. (*Infra* § 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1050-1063)).

Response to Finding No. 460

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

461. Many employees with administrative rights to their computers had unrestricted access to the Internet. (*Infra* § 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1058-1060)).

Response to Finding No. 461

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

462. Users with administrative rights to their computers could install software on their computers. (*Infra* § 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1056-1058)).

Response to Finding No. 462

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

463. Intentionally left blank.

464. Intentionally left blank.

4.2.4.2 LabMD Did Not Enforce Its Policy To Detect And Remove Unauthorized Applications

465. LabMD's Policy Manual includes a Software Monitoring Policy. (CX0006 (LabMD Policy Manual) at 18).

Response to Finding No. 465

Respondent has no specific response.

466. The Software Monitoring Policy states that the "'add/remove' programs file will be reviewed for the appropriate applications for the specific user." (CX0006 (LabMD Policy Manual) at 18).

Response to Finding No. 466

Respondent has no specific response.

467. LabMD affirmed that the Software Monitoring Policy went into effect in the second quarter of 2002, and was in effect during the 2007-2008 time frame. (CX0445 (LabMD Access Letter Response by P. Ellis, Jul. 16, 2010) at 6, 9 ("20. Software Monitoring Policy"); CX0446 (LabMD Access Letter Response by P. Ellis, Aug. 30, 2010) at 2, 6).

Response to Finding No. 467

Respondent has no specific response.

468. LabMD IT employees testified that they did not proactively inspect employee workstation computers for unauthorized applications using the "add/remove" programs function. (*Infra* § 5.3.2.3.1 (LabMD IT Employees Performed Manual Inspections Only on Request When Employee Workstations Malfunctioned) (¶¶ 668-671, 675-678)).

Response to Finding No. 468

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

469. Despite the Software Monitoring Policy that LabMD contends was being followed, LabMD did not detect that the LimeWire application had been downloaded to the Billing Computer without a business need, or prevent its use. (CX0730 (Simmons, Dep. at 53-56); CX0734 (Simmons, IHT at 160-61); CX0735 (Kaloustian, IHT at 269-70); CX0719 (Hyer, Dep. at 27-29, 33-34); *infra* § 8.1.2 (1718 File Shared on Gnutella Network Through LimeWire on a LabMD Billing Computer) (¶¶ 1363-1365, 1371-1372)).

Response to Finding No. 469

Respondent has no specific response.

470. Had LabMD implemented policies to identify and remove unauthorized applications, it would have discovered the LimeWire application installed on the computer used by LabMD's billing manager. (CX0740 (Hill Report) ¶ 61(b); *infra* § 5.3.2.3.5 (LabMD's Manual Inspections Did Not Detect the LimeWire Application Installed on the Computer Used By Lab MD's Billing Manager) (¶¶ 691-696)).

Response to Finding No. 470

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

471. As a result, between 2005 or 2006 and 2008, an employee with access to sensitive Personal Information of hundreds of thousands of consumers installed and used an unauthorized P2P file sharing program. (CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) at 4, Resp. to Interrog. 3 (LimeWire was downloaded to a LabMD computer in or about 2005); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 35-36, 40-41, 43-46; *infra* § 8.1.2 (1718 File Shared on Gnutella Network Through LimeWire on a LabMD Billing Computer) (¶¶ 1363-1372)).

Response to Finding No. 471

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The discovery responses indicate that a P2P program was downloaded and installed on a computer used by a billing manager, but they do not establish that this program was installed by that manager. Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

472. Intentionally left blank.

473. Intentionally left blank.

4.2.4.3 LabMD Did Not Enforce Its Recommendation That Employees Encrypt Emails

474. LabMD's Policy Manual and Computer Hardware, Software and Data Usage and Security Policy Manual include an Email Security and Encryption policy that recommends that employees encrypt emails containing sensitive information. (CX0006 (LabMD Policy Manual) at 6); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 7-8).

Response to Finding No. 474

Respondent has no specific response.

475. Encryption is a process for taking plain text data and making it unreadable by individuals who do not have access to the encryption key, which is a numeric value used as part of an algorithm to transform data into something that is not humanly readable. (Hill, Tr. 117-18).

Response to Finding No. 475

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

476. LabMD affirmed that this policy went into effect in the second quarter of 2004, and was in effect during the 2007-2008 time frame. (CX0445 (LabMD Access Letter

Response by P. Ellis, Jul. 16, 2010) at 4, 9 ("1. Acceptable Use and Security Policy"); CX0446 (LabMD Access Letter Response by P. Ellis, Aug. 30, 2010) at 2, 6).

Response to Finding No. 476

Respondent has no specific response.

477. LabMD had no such policy from at least 2004 through August 2009. (CX0711 (Dooley, Dep. at 12-13, 107-08); CX0735 (Kaloustian, IHT at 7, 277-80); CX0734 (Simmons, IHT at 163)).

Response to Finding No. 477

Respondent has no specific response.

478. Further, LabMD did not provide employees with any tools listed in its recommendation, such as S/MIME or PGP, to encrypt emails containing sensitive information. (CX0711 (Dooley, Dep. at 107-08); CX0707 (Bureau, Dep. at 87-88); CX0713-A (Gardner, Dep. at 62); CX0718 (Hudson, Dep. at 189); CX0735 (Kaloustian, IHT at 278); CX0734 (Simmons, IHT at 163); CX0722 (Knox, Dep. at 89-90); CX0709 (Daugherty, Dep. at 116-18); CX0713-A (Gardner, Dep. at 62)).

Response to Finding No. 478

Respondent has no specific response.

479. Nor did LabMD train employees on how to secure sensitive information in email or attachments. (CX0711 (Dooley, Dep. at 107-08); CX0707 (Bureau, Dep. at 87-88); CX0713-A (Gardner, Dep. at 62); CX0718 (Hudson, Dep. at 189)).

Response to Finding No. 479

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Complaint Counsel relies on testimony from Mr. Dooley, Mr. Bureau, Ms. Gardner, and Mr. Hudson. None of these witnesses testify as to whether LabMD "train[ed]" employees on how to secure sensitive information in email. All four witnesses were asked whether LabMD had a policy requiring encryption and whether employees were provided tools for encryption, but none of them were asked about LabMD's training regarding "secur[ing] sensitive information in email or attachments."

480. From at least 2004 through October 2006, sensitive information extracted from LabMD databases, such as billing information and insurance codes, was sent unencrypted from LabMD to Daugherty's personal AOL email account. (CX0711 (Dooley, Dep. at 107)).

Response to Finding No. 480

Respondent objects to this proposed finding of fact because Mr. Dooley's cited testimony does not indicate the information sent to Mr. Daugherty was sensitive.

Q. What kind of information did you send to his email address?

A. Sometimes I would do reports of miscellaneous things, just extraction from database – billing, insurance company codes. It's hard to recall specifics.

(CX0711 (Dooley, Dep. at 107)).

481. Intentionally left blank.

482. Intentionally left blank.

4.3 LabMD Did Not Use Reasonable, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities

4.3.1 Risk Assessment Is a Critical Component of a Comprehensive Information Security Plan

483. Risk assessment is an essential component of a layered security strategy. (CX0740 (Hill Report) ¶¶ 63-64).

Response to Finding No. 483

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009)(commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

484. Risk assessment in the IT field is the process of using readily available measures to identify commonly known or reasonably foreseeable security vulnerabilities on a network. (CX0740 (Hill Report) ¶ 64).

Response to Finding No. 484

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

485. The relationship between risk assessments and reasonable security is very well known among IT practitioners, and IT practitioners consider risk assessment the foundation for choosing security measures that are reasonable under their circumstances. (CX0740 (Hill Report) ¶ 64).

Response to Finding No. 485

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

486. When an assessment is inadequate or incomplete, network administrators and users may not know which risks or vulnerabilities they face and thus the security measures they should consider implementing. (CX0740 (Hill Report) ¶ 64).

Response to Finding No. 486

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

487. Intentionally left blank.

488. Intentionally left blank.

4.3.1.1 Frameworks for Conducting Risk Assessment Were Widely Available to LabMD

489. Frameworks for conducting risk assessments are widely available from many sources. (CX0740 (Hill Report) ¶ 64, 74).

Response to Finding No. 489

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

490. 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. (CX0740 (Hill Report) ¶ 74 and n. 25 (referring to CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002), which sets out risk assessment and risk mitigation methodologies); CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002) at 8).

Response to Finding No. 490

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)). Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re*

Realcomp II, Ltd., 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

491. 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. (CX0400 (NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems)) at 15-26).

Response to Finding No. 491

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> “These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis.”

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

492. These primary steps included methods and tools that could be used to perform them. (CX0400 (NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems)) at 15-26. For example, “Step 3: Vulnerability Identification” defined the term vulnerability and recommended gathering information about known vulnerabilities in programs running on a network, such as from prior risk assessments, vulnerability databases, and warnings from program vendors, and testing for the presence of the vulnerabilities, such as by penetration testing or otherwise. (CX0400 (NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems)) at 22-24).

Response to Finding No. 492

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

493. 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. (CX0740 (Hill Report) ¶ 74 (referring to CX0405 (HIPAA Security Series 6 – Basics of Risk Analysis And Risk Management) at 3, 5)).

Response to Finding No. 493

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "To be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014).

Furthermore, Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST regarding implementation of the HIPAA Security Rule, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

Moreover, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

494. The System Administration, Networking, and Security Institute ("SANS") provides security training and materials to practitioners who maintain and operate computer systems. (CX0738 (Shields Rebuttal Report) ¶ 40).

Response to Finding No. 494

Respondent objects to this proposed finding of fact because it is not specific to time a frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

495. Another source of vulnerability information is the Global Information Assurance Certification organization ("GIAC"). (CX0738 (Shields Rebuttal Report) ¶¶ 42-44).

Response to Finding No. 495

Respondent objects to this proposed finding of fact because it is not specific to a time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the*

Matter of LabMD, Inc., FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "In addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

496. These organizations publish information about particular risks and vulnerabilities and make the information public. (CX0738 (Shields Rebuttal Report) ¶ 40).

Response to Finding No. 496

Respondent objects to this proposed finding of fact because it is not specific to a time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "In addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

497. Intentionally left blank.

498. Intentionally left blank.

4.3.1.2 Warnings and Comprehensive Information About Known or Reasonably Foreseeable Vulnerabilities Were Readily Available to LabMD from Government and Private Sources

499. Many sources of information about vulnerabilities that may be present on a network are freely available, including vulnerability libraries, security requirements checklists, and training materials and classes. (CX0740 (Hill Report) at 62-66; CX0738 (Shields Rebuttal Report) ¶¶ 40-49; CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002) at 23-24).

Response to Finding No. 499

Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying training materials, security requirements checklists and vulnerabilities libraries, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)). Furthermore, Respondent objects to this proposed finding of fact because it contains expert opinion or conclusion, and thus is not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used

500. The information technology industry has systematically compiled information about known vulnerabilities in publicly-available vulnerability libraries. (CX0740 (Hill Report) at 62-66; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19-35). Public vulnerability libraries inform IT practitioners and users about known vulnerabilities and how to remove or mitigate them. (CX0740 (Hill Report) ¶ 72 and at 62-66; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19-35).

<u>Response to Finding No. 500</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

501. Publicly available vulnerability libraries include: the Common Vulnerabilities and Exposures ("CVE"); Common Vulnerability Scoring System ("CVSS); National Vulnerability Database ("NVD"), and US Computer Emergency Response Team ("US-CERT"). (CX0740 (Hill Report) at 62-66; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19-35).

Response to Finding No. 501

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

502. CVE is a dictionary that tracks information about known network and information security vulnerabilities, assigning each an identifier and providing information about the vulnerability. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 41). CVE is free and is sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security, and is operated by the Mitre Corporation. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, which links to http://cve.mitre.org, which, in turn, links to FAQ A6)).

Response to Finding No. 502

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

503. The CVSS framework calculates numerical scores for vulnerabilities that range from 0.0 to 10.0, with 10.0 being the most severe. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, which links to "Impact Metrics")). The scores take into account a number of factors, including: how easy or hard it is to exploit a particular vulnerability (attack complexity) and the extent of the impact of exploitation on confidentiality, integrity, and availability. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (link to the number identified as the "CVSS v2 Base Score" for an FTP vulnerability and then the associated "Base Score Metrics" section))).

Response to Finding No. 503

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

504. A vulnerability's CVSS numerical severity score classifies the extent of the vulnerability's impact on confidentiality, integrity, and availability as "complete," "partial," or "none." (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 and link to "legend" associated with the "CVSS v2 Base Score")).

Response to Finding No. 504

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

505. A complete confidentiality impact means that: "[t]here is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.)." (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (link to "10.0" associated with "CVSS v2 Base Score" and, in the "Impact Metrics" section of the "Base Score Metrics" section, put the cursor on "Complete (C:C)")).

Response to Finding No. 505

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

506. A complete integrity impact means that: "[t]here is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system." (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (link to "10.0" associated with "CVSS v2 Base Score" and, in the "Impact Metrics" section of the "Base Score Metrics" section, put the cursor on "Complete (I:C)")).

Response to Finding No. 506

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

507. A complete availability impact means that: "[t]here is a total shutdown of the affected resource. The attacker can render the resource completely unavailable." (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (link to "10.0" associated with "CVSS v2 Base Score" and, in the "Impact Metrics" section of the "Base Score Metrics" section, put the cursor on "Complete (A:C)")).

Response to Finding No. 507

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

508. The CVSS framework also includes a calculator that an entity can use to adjust a vulnerability's base CVSS score to take into account the entity's "environmental" circumstances, that is, details about its IT system that may affect the CVSS score. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (link to "10.0" associated with "CVSS v2 Base Score" and put the cursor on "Environmental Score Metrics" section)).

Response to Finding No. 508

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

509. The NVD is the U.S. government repository of standards based vulnerability management data that enables automation of vulnerability management, security measurement, and compliance. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527 (particular vulnerability that was found in the FTP application LabMD used))). NVD is the CVE dictionary augmented with additional analysis, a database, and a search engine. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, which links to FAQ 1)). The entire NVD can be downloaded for public use. (CX0740 (Hill Report) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, which links to "Data Feeds")). NVD provides severity rankings of 'Low,' 'Medium,' and 'High' based on the numeric CVSS scores. (CX0740 (Hill Report) at 63 (citing NVD, (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0527, which includes a link to "Impact Metrics")).

Response to Finding No. 509

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

510. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) distributes vulnerability and threat information through its National Cyber Awareness System (NCAS), and operates a Vulnerability Notes Database to provide technical descriptions of system vulnerabilities. (CX0740 (Hill Report) at 63, (citing The Computer Emergency Response Team (CERT) -- Anonymous FTP Activity (1997), http://www.cert.org/historical/advisories/CA-1993-10.cfm, which links to "Advisories" (noting that CERT advisories are now part of US-CERT))). US-CERT collaboratively responds to incidents, provides technical assistance to information system operators, and disseminates notifications regarding current and potential security threats and vulnerabilities. (CX0740 (Hill Report) at 63 (citing The Computer Emergency Response Team (CERT) -- Anonymous FTP Activity (1997), http://www.cert.org/historical/advisories/CA-1993-10.cfm, which links to "Advisories" (noting that CERT advisories are now part of US-CERT))).

Response to Finding No. 510

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

511. A number of organizations provide training security materials and classes for practitioners, including SANS. (CX0738 (Shields Rebuttal Report) ¶¶ 40-48).

Response to Finding No. 511

Respondent objects to this proposed finding of fact because it is not specific to a time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "In addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case."). Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

512. For years, LabMD did not consult such sources to learn about vulnerabilities to look for on its network. (CX0735 (Kaloustian, IHT at 123-24)).

Response to Finding No. 512

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

513. Intentionally left blank.

4.3.1.3 Many Tools Are Available to Assess and Remediate Risks

514. IT practitioners use a variety of measures and techniques to assess and remediate risks, including antivirus applications, firewalls, vulnerability scans, intrusion detection systems, penetration tests, and file integrity monitoring. Each mechanism assesses for vulnerability or exposure to a particular type of risk, and no one mechanism can assess the exposure to all the risks and vulnerabilities a network may face. (CX0740 (Hill Report) ¶ 65). A reasonable risk assessment process usually requires the use of a number of mechanisms. (CX0740 (Hill Report) ¶ 65).

Response to Finding No. 514

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

515. For example, antivirus applications can assess the incidence of viruses on a network, but not the installation of unauthorized applications on the network, while external vulnerability scans can assess the incidence of vulnerabilities in an application inside the network, but not the incidence of viruses. (CX0740 (Hill Report) ¶ 65).

Response to Finding No. 515

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

516. Likewise, file integrity monitoring can identify changes in critical files that may indicate malware has been installed on the network, but does not identify or remove the malware. (CX0740 (Hill Report) ¶ 65).

Response to Finding No. 516

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

517. Network administrators usually have a number of options to choose from in each mechanism category. (CX0740 (Hill Report) ¶ 66). For example, there are a number of branded antivirus applications, and within a brand there often are versions that differ in cost, the types of functions they can perform, and other aspects of performance. (CX0740 (Hill Report) ¶ 66).

Response to Finding No. 517

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

518. Having options provides companies with flexibility, so that they can balance the effectiveness of a mechanism, the sensitivity of the business and consumer information the assessment concerns, and the mechanism's cost. (CX0740 (Hill Report) ¶ 66).

Response to Finding No. 518

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

519. LabMD relied on antivirus software, firewalls, and manual computer inspections to assess risks on its network. These mechanisms were not sufficient to identify or assess risks and vulnerabilities to the Personal Information maintained on LabMD's network. (CX0740 (Hill Report) ¶ 68; *infra* § 5.3.2 (LabMD Could Not Effectively Assess Risks Using Only Antivirus Applications, Firewalls, and Manual Inspections) *et seq.* (¶¶ 524-696)).

Response to Finding No. 519

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

520. For example, LabMD did not use an intrusion detection system or file integrity monitoring, and did not perform penetration testing until 2010. (*Infra* §§ 5.3.3.1 (LabMD Did Not Implement an Intrusion Detection System ("IDS") or Intrusion Protection System ("IPS") (¶¶ 699-702), 5.3.3.2 (LabMD Did Not Implement File Integrity Monitoring) (¶¶ 705-712), 5.3.4 (LabMD Did Not Use Penetration Testing Before 2010) (¶¶ 715-726)). Without automated mechanisms, such as IDS, file integrity monitoring, and penetration testing, LabMD could not adequately assess the extent of the risks and vulnerabilities on its network. (CX0740 (Hill Report) ¶ 69).

Response to Finding No. 520

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of*

LabMD, Inc., FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

521. LabMD did not use a reasonable set of readily available measures to assess risks and vulnerabilities to the Personal Information within its computer network during the Relevant Time Period. (CX0740 (Hill Report) ¶ 67).

Response to Finding No. 521

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

522. Intentionally left blank.

523. Intentionally left blank.

4.3.2 LabMD Could Not Effectively Assess Risks Using Only Antivirus Applications, Firewalls, and Manual Inspections

524. The mechanisms LabMD used for risk assessment prior to 2010 – antivirus applications, firewalls, and manual computer inspections – were not sufficient to identify or assess risks and vulnerabilities to the Personal Information maintained on Lab MD's computer network. (CX0740 (Hill Report) ¶ 68; *infra* §§ 5.3.2.1 (LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans) *et seq.* (¶¶ 527-629), 5.3.2.2 (LabMD's Firewall Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 631-657), 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 660-696)).

Response to Finding No. 524

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

525. Intentionally left blank.

526. Intentionally left blank.

4.3.2.1 LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans

527. Antivirus software detects the presence of malicious software. (Hill, Tr. 108; Hill, ¶ 31(e)).

Response to Finding No. 527

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

528. LabMD has used several antivirus applications since 2005 on its workstations, servers, and computers supplied to physician-clients. (CX0711 (Dooley, Dep. at 72-73, 75) (ClamWin); CX0735 (Kaloustian, IHT at 43-44, 126-27, 130 (ClamWin), 187-88 (Trend Micro)); CX0734 (Simmons, IHT at 60, 70-71, 87, 115-16 (AVG)); CX0552 (Simmons Network Diagram); CX0707 (Bureau, Dep. at 43, 45 (AVG and Trend Micro)); CX0705-A (Bradley, Dep. at 82-83 (Trend Micro, AVG))).

Response to Finding No. 528

Respondent has no specific response.

529. Antivirus updates include loading new virus definitions that are needed to identify whether newly discovered viruses are present. A virus's signature is unique to that specific virus. If antivirus software cannot or does not update to get new signatures, then it cannot detect the new and emerging viruses that may be present on a system. (CX0740 (Hill Report) ¶ 68(a); Hill, Tr. 147; CX0735 (Kaloustian, IHT at 127-28)).

Response to Finding No. 529

Respondent objects to this proposed finding of fact because it contains expert opinion or conclusion, and thus is not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

530. During the relevant time period, LabMD's security contractor's practice was to use up-to-date, current antivirus software on its client's computers. (CX0731 (Truett, Dep. at 45); CX0035 (Automated PC Technologies, Inc. ("APT") Service Invoice) at 2, 3, 5).

Response to Finding No. 530

Respondent has no specific response.

531. At times, LabMD failed to update virus definitions. (*Infra* §§ 5.3.2.1.1.1 (LabMD Did Not Consistently Update Symantec Virus Definitions on Servers) (¶¶ 539-550), 5.3.2.1.2.1 (LabMD Did Not Consistently Update Virus Definitions on Employee Computers) *et seq*. (¶¶ 566-587), 5.3.2.1.3.1 (LabMD Did Not Consistently Update Virus Definitions On Computers Provided To Physician-Clients' Offices) (¶¶ 612-618)).

Response to Finding No. 531

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

532. The purpose of antivirus software is to detect the presence of malicious software or an attack while it is occurring. (CX0740 (Hill Report) ¶ 31(e)).

<u>Response to Finding No. 532</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

533. Therefore, along with timely updating virus definitions, effectively using antivirus programs requires running virus scans to identify risks and then reviewing the scans to identify viruses that need to be corrected. (CX0740 (Hill Report) ¶¶ 66, 68(a); Hill, Tr. 145-49).

<u>Response to Finding No. 533</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

534. At times, LabMD failed to run virus scans. (*Infra* §§ 5.3.2.1.1.2 (LabMD Did Not Consistently Run Symantec Antivirus Scans on Servers) (¶¶ 553-558), 5.3.2.1.2.2 (LabMD Did Not Consistently Run Antivirus Scans on Employee Computers *et seq.* (¶¶ 590-601)), 5.3.2.1.3.2 (LabMD Did Not Consistently Run Antivirus Scans of Computers Provided to Physician-Clients) (¶¶ 621-623)).

Response to Finding No. 534

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

535. Even where scans were run, LabMD reviewed antivirus scans only in response to complaints. (*Infra* §§ 5.3.2.1.1.3 (LabMD Did Not Consistently Review Symantec Antivirus Scans Run on Servers) (¶¶ 561-563), 5.3.2.1.2.3 (LabMD Did Not Consistently Review Antivirus Scans Run on Employee Computers) (¶¶ 604-609), 5.3.2.1.3.3 (LabMD Did Not Consistently Review Antivirus Scans Run on Computers Provided to Physician-Clients) (¶¶ 626)).

Response to Finding No. 535

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

536. After a scan was run and a virus detected, LabMD's antivirus software did not have the capability to remediate the problem and remove the virus. (CX0735 (Kaloustian, IHT at 135)). IT staff had to seek out a cleaner application for the particular virus identified. (CX0735 (Kaloustian, IHT at 135); CX0734 (Simmons, IHT at 72)).

Response to Finding No. 536

Respondent objects to this proposed finding of fact to the extent it relies upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, In the Matter of LabMD, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."). Respondent further objects to this proposed finding of fact because it is not specific to time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, In the Matter of LabMD, Inc., FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "In addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case. "Ms. Simmons testified that she would use "various anti-spyware, antivirus" to remove viruses from infected computers. (CX0734 Simmons Dep. at 72)).

537. Intentionally left blank.

538. Intentionally left blank.

4.3.2.1.1 On Servers, LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans

4.3.2.1.1.1 LabMD Did Not Consistently Update Symantec Virus Definitions on Servers

539. Between 2004 and 2006, LabMD used the Norton antivirus application, also known as Symantec, on its servers. (CX0717 (Howard, Dep. at 61, 70-71)).

Response to Finding No. 539

Respondent has no specific response.

540. LabMD used its servers to receive sensitive information about hundreds of thousands of consumers from physician clients using computers LabMD operated in client offices. (*Supra* §§ 4.7.3.2.1 (Mapper Server) (¶¶ 220-224), 4.7.3.2.2 (LabNet Server) (¶¶ 225-233); 4.7.3.2.3 (Lytec Server) (¶¶ 235-240).

Response to Finding No. 540

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

541. Symantec was supposed to update virus definitions automatically; however, LabMD had no process to ensure that Symantec updated automatically and functioned properly between 2005 and early 2007. (CX0717 (Howard, Dep. at 63)).

Response to Finding No. 541

Respondent objects to this proposed finding of fact because it is an attempt to mislead the Court by stating that LabMD had **no process** to ensure proper operation of its antivirus software despite clear evidence in the record to the contrary. APT provided services to LabMD from "2001 or 2002 to 2008 or 2009" (CX 0731 (Truett, Dep. at 25, 72-73)). Its owner Allen Truett testified that his staff on a monthly basis conducted "Backup log checks monthly-antivirus report on servers." (CX0731 (Truett Dep. at 32-33.))

542. While LabMD's servers had antivirus applications installed on them, between 2006 and 2009 many of the servers did not have Internet connections to use to update virus definitions automatically. (CX0735 (Kaloustian, IHT at 91-92)).

Response to Finding No. 542

Respondent objects to this proposed finding of fact to the extent it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

543. Information was passed between servers on LabMD's internal network. (*See, e.g.*, *supra* § 4.7.3.2.1 (Mapper Server) (¶¶ 220-221)).

Response to Finding No. 543

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

544. An outside security provider found that a LabMD server had not updated its antivirus definitions between July 2005 and May 3, 2006. (CX0035 (Automated PC Technologies, Inc. ("APT") Service Invoice) at 2); CX0731 (Truett, Dep. at 142-43)).

Response to Finding No. 544

APT Service Invoice indicated that LabMD's server had not updated since July of 2005. However, Mr. Truett clearly testified—in the citation provided by Complaint Counsel—

that he “can’t say for sure” whether that “mean[s] that as of the date of that entry, which is May 3rd, 2006, it would not have updated antivirus definitions since July 2005.” Rather, Mr. Allen explained, “[i]t could be that the antivirus definition reverted back to that July 2005 date, and, you know, subsequently it did have virus updates. I would say from that statement you can’t be certain of that.” (CX0731 (Truett, Dep. at 143)).

545. On May 3, 2006, the LabMD server would not get updates for virus definitions. (CX0035 (APT Service Invoice) at 2).

Response to Finding No. 545

Respondent objects to this proposed finding of fact because it is merely a statement contained in the APT Service Invoice and is only probative of the fact that this statement was contained in the APT Service Invoice and therefore should be accorded little weight as to its truth or accuracy.

546. As of June 21, 2006, LabMD’s servers had not been updating antivirus definitions since May 2006. (CX0035 (APT Service Invoice) at 3); CX0731 (Truett, Dep. at 83-84)).

Response to Finding No. 546

Respondent has no specific response.

547. On June 21, 2006, LabMD was running Symantec on its servers. (CX0035 (APT Service Invoice) at 3; CX0731 (Truett, Dep. at 81-82)).

Response to Finding No. 547

Respondent has no specific response.

548. At that time, Symantec was not supported by the vendor, which had stopped providing virus definition updates needed to identify newly discovered risks. (CX0398 (APT Service Invoice) at 3; CX0731 (Truett, Dep. at 82-84); *see also* CX0740 (Hill Report) ¶ 68(a)).

Response to Finding No. 548

Respondent objects to this finding of fact because it is unsupported by the record. The citation to page 3 of CX0398 contains no statement that Symantec was not supported by the vendor on June 21, 2006, or that Symantec had stopped providing virus definition updates needed to identify newly discovered risks. Mr. Truett does not testify to this claim, either. In fact, Mr. Truett specifically answers "I don't know in the case of Symantec" when he was asked, "[d]oes it mean that virus updates would still be available or no?" (CX0731 (Truett, Dep. at 82-84)). Ms. Hill's report does not address whether Symantec was supported by the vendor and whether the vendor continued to provide virus updates.

549. On or about June 21, 2006, APT suggested that LabMD upgrade its antivirus application because its current application was not updating virus definitions. (CX0035 (APT Service Invoice) at 3; CX0731 (Truett, Dep. at 84)).

Response to Finding No. 549

Respondent has no specific response.

550. LabMD did not have new antivirus software installed until November 2006. (CX0731 (Truett, Dep. at 79-80)).

Response to Finding No. 550

Respondent has no specific response.

551. Intentionally left blank.

552. Intentionally left blank.

4.3.2.1.1.2 LabMD Did Not Consistently Run Symantec Antivirus Scans on Servers

553. The antivirus application LabMD used on critical servers did not always scan for viruses. (CX0035 (APT Service Invoice) at 2; CX0398 (APT Service Invoice) at 4).

Response to Finding No. 553

Respondent objects to this proposed finding of fact because it is merely a statement contained in the APT Service Invoice and is only probative of the fact that this statement was contained in the APT Service Invoice and therefore should be accorded little weight as to its truth or accuracy.

554. For example, on May 3, 2006, the LabMD server would not run a virus scan. (CX0035 (APT Service Invoice) at 2).

Response to Finding No. 554

Respondent objects to this proposed finding of fact because it is merely a statement contained in the APT Service Invoice and is only probative of the fact that this statement was contained in the APT Service Invoice and therefore should be accorded little weight as to its truth or accuracy.

555. The servers' antivirus program did not automatically scan for viruses or perform regular scans between 2006 and 2009. (CX0735 (Kaloustian, IHT at 91)).

Response to Finding No. 555

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."

556. Between 2006 and 2009, antivirus was deployed only after a problem was observed. (CX0735 (Kaloustian, IHT at 91-92)).

Response to Finding No. 556

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing

Conference, In the Matter of LabMD, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."

Respondent also objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited portions of Mr. Kaloustian's testimony not only fail to support Complaint Counsel's proposed finding of fact, it directly contradicts it. Mr. Kaloustian actually testified as follows:

> Q. I'm going to go through a series of different concepts that might be used that we can talk about in terms of risks. And so again, I just want a general big picture here, how did the company assess risks for viruses, for example?
>
> A. They wouldn't. They were reactive to those kind of issues, like most of the other IT issues. We did not have tools to basically monitor networks, monitor viruses early on. The antivirus freeware application that we used when I first got there that we put on all desktops, servers, and whatnot was woefully inadequate.

(CX0735 (Kaloustian, IHT at 91-92)).

In addition to the above objections, there is direct, contradictory evidence in the record. Mr. Jeremy Dooley testified as follows:

> Q. (By Mr. Sheer) I want to turn to the antivirus applications. Do you know which antivirus applications LabMD used while you worked at the company?
>
> MS. HARRIS: Objection: Calls for speculation, over broad, vague and ambiguous.
>
> A. Do you want me to make a stab at it?

> Q. (By Mr. Sheer) Let me give some examples and maybe you can respond and tell me if you recognize them. Semantec Corporate 7?
>
> MS. HARRIS: Objection: Over broad as to time frame. What is the question?
>
> Q. (By Mr. Sheer) I'm asking whether Semantec Corporate 7 was one of the antivirus applications while you worked there.
>
> A. I do remember there were two different eras as far as LabMD locations. There was preAPT and then postAPT. When APT came along, they did install essentially managed antivirus software. I think we had another centrally managed antivirus software prior to that, and I think that was Norton. APT may have installed Symantec because that was whatever their preference was. As far as work stations that were at client locations, they also went out from our location with antivirus software installed, and it was–there was a variety of different applications or different antivirus softwares. They couldn't be centrally managed. They were off site. We would get these communities computers from Dell, and they would come with antivirus software preinstalled. In the occasions they weren't, we would install it.

CX0711 (Dooley, Dep. at 71-72)). LabMD IT employee Dooley started with LabMD in November of 2004 and ended his employment with LabMD in December 2006. (CX711 (Dooley, Dep. at 12-13)).

557. LabMD did not have tools to monitor the network for viruses as of October 2006. (CX0735 (Kaloustian, IHT at 91)).

<u>Response to Finding No. 557</u>

Respondent objects to this proposed finding of fact because it is an attempt to mislead the Court despite clear evidence in the record to the contrary, by stating that LabMD did not have tools to monitor its network for viruses. It is clear from the evidence in the record that LabMD had antivirus software prior to October 2006. LabMD IT employee Dooley started with LabMD in November of 2004 and ended his employment with LabMD in December 2006. (CX711 (Dooley, Dep. at 12-13)). Dooley testified that at that time LabMD was concerned with viruses as every organization was. He stated LabMD installed Norton antivirus software and later APT installed Symantec antivirus software. (CX0711 (Dooley, Dep. at 30-31 and 71-72)).

Furthermore, Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."

558. The only way LabMD IT employees would have been able to identify if a virus had entered the system would have been to see the effects and then react to scrub clean the virus from the system. (CX0735 (Kaloustian, IHT at 91-92)).

Response to Finding No. 558

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, In the Matter of LabMD, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel’s use of Kaloustian testimony, this Court stated “… [investigational hearing depositions are] taken without counsel, without respondent present, don’t expect them to be given a lot of weight in this proceeding.”

In addition, Respondent objects to this proposed finding of fact as there is direct, contradictory evidence in the record. Specifically, Robert Hyer testified that he performed regular, manual and automated checks and inspections on all LabMD computers after July 2009. (CX0719 (Hyer, Dep. at 96-99)).

559. Intentionally left blank.

560. Intentionally left blank.

4.3.2.1.1.3 LabMD Did Not Consistently Review Symantec Antivirus Scans Run on Servers

561. Between 2004 and 2006, warnings or reports were only provided by Symantec on LabMD servers upon request by IT employees. (CX0717 (Howard, Dep. at 63, 64, 70-71)).

<u>Response to Finding No. 561</u>

Respondent has no specific response.

562. Reports or warnings by Symantec on LabMD servers were only requested and examined when there was a problem reported by an individual user. (CX0717 (Howard, Dep. at 63-65)).

<u>Response to Finding No. 562</u>

Respondent has no specific response.

563. When an individual user reported a problem with their computer at LabMD, such as it freezing or not properly loading a website, a LabMD IT employee would examine the reports in Symantec to see if any items were quarantined and when the last scan was run, and then run a manual scan. (CX0717 (Howard, Dep. at 65-66)).

<u>Response to Finding No. 563</u>

Respondent has no specific response.

564. Intentionally left blank.

565. Intentionally left blank.

4.3.2.1.2 On Employee Computers, LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans

4.3.2.1.2.1 LabMD Did Not Consistently Update Virus Definitions on Employee Computers

4.3.2.1.2.1.1 Employees Did Not Consistently Update ClamWin Virus Definitions on Their Computers

566. ClamWin was free, open source antivirus software. (CX0711 (Dooley, Dep. at 72-73)).

Response to Finding No. 566

Respondent has no specific response.

567. ClamWin virus definitions were not automatically updated on employee computers between October 2006 until it was replaced with a new antivirus program on employee computers in approximately late 2007. (CX0735 (Kaloustian, IHT at 127-28, 130); CX0616 (Email C. Maire to J. Boyle Subject: TrendMicro, with Notes)).

Response to Finding No. 567

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus LabMD employees would have no responsibilities for updating it. (CX0711 (Dooley, Dep. at 75-76; (CX0724 (Maire, Dep. at 95-96)).

568. ClamWin was not managed centrally by a network administrator, and required individual updates to each computer. (CX0735 (Kaloustian, IHT at 126-32)).

Response to Finding No. 568

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

569. Central management allows IT employees to remotely update antivirus applications and virus definitions on employee computers, run antivirus scans, review scan results, and take corrective action. (CX0740 (Hill Report) ¶ 68(a); CX0735 (Kaloustian, IHT at 127-30, 135, 140)).

Response to Finding No. 569

Respondent objects to this proposed finding of fact as it relies upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

Respondent further objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

570. Without central management, individual employees had to update the virus definitions on their computers and report warnings to LabMD's IT Department.

(*Infra* ¶¶ 573-574, §§ 5.3.2.1.2.2 (LabMD Did Not Consistently Run Antivirus Scans on Employee Computers) *et seq*. (¶¶ 591-593, 600-601), 5.3.2.1.2.3 (LabMD Did Not Consistently Review Antivirus Scans Run on Employee Computers) (¶¶ 604-609); CX0740 (Hill Report) ¶ 68(a)).

<u>Response to Finding No. 570</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

571. LabMD's IT Department employees did not always update ClamWin virus definitions on employee computers. (CX0735 (Kaloustian, IHT at 130)).

<u>Response to Finding No. 571</u>

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus LabMD employees would have no responsibilities for it. (CX0711 (Dooley, Dep. at 75-76; (CX0724 (Maire, Dep. at 95-96)).

Furthermore, Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

572. LabMD did not provide any information security training to its employees. (*Infra* § 5.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information) *et seq.* (¶¶ 866-900).

Response to Finding No. 572

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite Jto specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

573. Yet LabMD relied on individual employees to update the virus definitions on their computers. (CX0735 (Kaloustian, IHT at 126-32)).

Response to Finding No. 573

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

574. ClamWin virus definitions could only be updated if an individual visited the ClamWin website and downloaded updated definitions. (CX0735 (Kaloustian, IHT at 127-28)).

<u>Response to Finding No. 574</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

575. Many employee computers did not have Internet connections needed to update virus definitions on the computers. (CX0735 (Kaloustian, IHT at 160-61)).

<u>Response to Finding No. 575</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

576. Employee computers not connected to the Internet nonetheless could get viruses through CDs and thumb drives. (CX0735 (Kaloustian, IHT at 135-36)).

Response to Finding No. 576

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

577. LabMD's IT Department did not regularly check to see if employees had updated ClamWin virus definitions on their computers. (CX0735 (Kaloustian, IHT at 129-30, 132)).

Response to Finding No. 577

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus LabMD employees would have no responsibilities for updating it. (CX0711 (Dooley, Dep. at 75-76; (CX0724 (Maire, Dep. at 95-96)). Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

578. Many LabMD employees did not update their ClamWin antivirus virus definitions. (CX0735 (Kaloustian, IHT at 128)).

Response to Finding No. 578

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus LabMD employees would have no responsibilities for updating it. (CX0711 (Dooley, Dep. at 75-76; (CX0724 (Maire, Dep. at 95-96)). Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

579. Intentionally left blank.

580. Intentionally left blank.

4.3.2.1.2.1.2 LabMD Had No Process To Verify That AVG Definitions Were Up-To-Date on Employee Computers

581. Another antivirus software LabMD used on employee computers was a free version of AVG antivirus software. (CX0734 (Simmons, IHT at 60, 159-60)).

Response to Finding No. 581

Respondent has no specific response.

582. Between October 2006 and October 2009, AVG did not have a central reporting or management. (CX0734 (Simmons, IHT at 89)).

Response to Finding No. 582

Respondent has no specific response.

583. While AVG was set up to automatically update virus definitions on employee computers, LabMD did not have a process or procedure for verifying that AVG virus definitions had been updated and were working. (CX0734 (Simmons, IHT at 92-93)).

Response to Finding No. 583

Respondent objects to this finding of fact because it is unsupported by the record. Ms. Simmons did not testify that "LabMD did not have a process or procedure for verifying that AVG virus definitions had been updated and were working." Rather, she testified, "**I don't know** that we had a procedure concerning that." (CX0734 (Simmons, IHT at 92-93)).

584. LabMD installed AVG antivirus on laptops. (CX0705-A (Bradley, Dep. at 82-83); CX0707 (Bureau, Dep. at 43, 45)).

Response to Finding No. 584

Respondent has no specific response.

585. The sales representatives' laptop computers could only automatically update programs when connected to the Internet. (CX0717 (Howard, Dep. at 91)).

Response to Finding No. 585

Respondent has no specific response.

586. Sales representatives could work offline. (CX0718 (Hudson, Dep. at 182)).

Response to Finding No. 586

Respondent has no specific response.

587. At least from 2004 through March 2007, LabMD IT personnel would only work on the laptop computer of a salesperson if the computer had a problem. (CX0717 (Howard, Dep. at 91-92)).

Response to Finding No. 587

Respondent has no specific response.

588. Intentionally left blank.

589. Intentionally left blank.

4.3.2.1.2.2 LabMD Did Not Consistently Run Antivirus Scans on Employee Computers

4.3.2.1.2.2.1 LabMD Employees Did Not Consistently Run ClamWin Scans, And LabMD Had No Process To Verify They Had Done So

590. ClamWin ran virus scans on demand, but did not perform real-time scanning. (CX0735 (Kaloustian, IHT at 126-27, 129)).

Response to Finding No. 590

Respondent objects to this proposed finding of fact because it is an attempt to mislead the Court despite clear evidence in the record to the contrary. Clam Win ran scans on a schedule. It also ran updates on a schedule to check for virus signatures in real time. (CX0711 (Dooley, Dep. at 75, 88); (CX0724 (Maire, Dep. at 95-96)).

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "…

[investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

591. LabMD relied on individual employees to run scans on their computers. (CX0735 (Kaloustian, IHT at 129)).

Response to Finding No. 591

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers used at client locations and thus LabMD employees would have no responsibilities for it. (CX0711 (Dooley, Dep. at 75-76)). Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

592. LabMD did not have a policy requiring employees to run ClamWin scans. (CX0735 (Kaloustian, IHT at 130)).

Response to Finding No. 592

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers used at client locations and thus LabMD employees would have no responsibilities for it. (CX0711 (Dooley, Dep. at 75-76); (CX0724 (Maire, Dep. at 95-96)).

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD,* FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

593. LabMD did not verify that employees had run antivirus scans. (CX0735 (Kaloustian, IHT at 131)).

<u>Response to Finding No. 593</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD,* FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

Respondent further objects to this finding of fact because it is unsupported by the citation to the record. Mr. Kaloustian only testified that LabMD did not verify that employees had run antivirus scans using ClamWin; he did not testify as to whether LabMD verified that employees ran scans generally. (CX0735 (Kaloustian, IHT at 131 – 132)).

594. [Former LabMD Employee] could not recall whether LabMD used any antivirus applications on her computer and she did not recall doing anything with an antivirus program on her computer. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 83)).

Response to Finding No. 594

Respondent has no specific response.

595. ClamWin was not an effective tool for cleaning viruses. Instead, when the ClamWin program found a virus on an employee's computer, LabMD's IT employees used other tools to clean the viruses. (CX0735 (Kaloustian, IHT at 135, 259-263)).

Response to Finding No. 595

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus ClamWin would not have found any viruses on LabMD employees' computers. (CX0711 (Dooley, Dep. at 75-76); (CX0724 (Maire, Dep. at 95-96)).

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

596. Because employees did not update virus definitions and run scans of their computers, the IT Department received many PCs from salespeople that had viruses and malware on them. (CX0735 (Kaloustian, IHT at 128)).

Response to Finding No. 596

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

Respondent further objects to this finding of fact because it is unsupported by the citation to the record. Mr. Kaloustian did not directly attribute the viruses and malware found on the salespeople's computers to their failure to update virus definitions. (CX0735 (Kaloustian, IHT at 128)).

597. Intentionally left blank.

598. Intentionally left blank.

4.3.2.1.2.2.2 LabMD Had No Process To Verify That AVG Was Scanning Employee Computers

599. AVG scans were set up to run at night, but were not real-time scans. (CX0734 (Simmons, IHT at 69-70)).

Response to Finding No. 599

Respondent has no specific response.

600. LabMD did not have a process for reviewing or verifying that AVG was operating properly on employee computers. (CX0734 (Simmons, IHT at 73, 93)).

Response to Finding No. 600

Respondent has no specific response.

601. The only way for LabMD's IT employees to learn that AVG was not working correctly was by complaints received from employees. (CX0734 (Simmons, IHT at 93)).

Response to Finding No. 601

Respondent has no specific response.

602. Intentionally left blank.

603. Intentionally left blank.

4.3.2.1.2.3 LabMD Did Not Consistently Review Antivirus Scans Run on Employee Computers

604. LabMD relied on individual employees to report warnings from antivirus programs to LabMD's IT Department. (CX0735 (Kaloustian, IHT at 126-32)).

Response to Finding No. 604

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

605. LabMD's IT employees only inspected employee computers when employees complained about the performance of their computers. (CX0734 (Simmons, IHT at 92-93)).

Response to Finding No. 605

Respondent objects to this proposed finding of fact because it is not specific to time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.”). Furthermore, Respondent objects to this finding of fact because it is unsupported by the citation to the record. Ms. Simmons did not testify as to the only time LabMD’s IT employees would inspect an employee computer. She was asked how LabMD would know if a specific antivirus program, AVG, had stopped working, and she indicated that the only way LabMD would acquire this information is if a user reported the problem. But she was not asked about the times in which IT personnel would inspect computers for reasons other than AVG not working.

606. AVG did not provide a warning to IT employees that it had found a problem on a computer; instead, a warning appeared only on the user’s computer screen. (CX0734 (Simmons, IHT at 89, 91)).

<u>Response to Finding No. 606</u>

Respondent has no specific response.

607. After seeing an AVG antivirus warning on their computer screens, employees would call the IT Department for help. (CX0734 (Simmons, IHT at 91-92)).

<u>Response to Finding No. 607</u>

Respondent has no specific response.

608. AVG did not have central logging capability. (CX0734 (Simmons, IHT at 99-100)).

<u>Response to Finding No. 608</u>

Respondent has no specific response.

609. Central logging capability is necessary because without it, individual employees had to update virus definitions on their computers and report warnings to LabMD’s IT department. (CX0740 (Hill Report) ¶ 68(a)).

<u>Response to Finding No. 609</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

610. Intentionally left blank.

611. Intentionally left blank.

4.3.2.1.3 On Computers Provided to Physician-Clients' Offices, LabMD's Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans

4.3.2.1.3.1 LabMD Did Not Consistently Update Virus Definitions on Computers Provided to Physician-Clients' Offices

612. From October 2006 until at least mid-2008, LabMD installed ClamWin on computers LabMD supplied to physician-client's offices. (CX0735 (Kaloustian, IHT at 147); CX0724 (Maire, Dep. at 95); CX0711 (Dooley, Dep. at 72-73, 75)).

<u>Response to Finding No. 612</u>

Respondent has no specific response.

613. LabMD did not control ClamWin updates on computers it supplied to physician-clients' offices. (CX0724 (Maire, Dep. at 96)).

<u>Response to Finding No. 613</u>

Respondent has no specific response.

614. ClamWin did not update virus definitions automatically. (*Supra* § 5.3.2.1.2.1.1 (Employees Did Not Consistently Update ClamWin Virus Definitions on Their Computers) (¶¶ 568-571)).

<u>Response to Finding No. 614</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record that Calm Win was only used on computers at client locations and thus LabMD employees would have no reason to update it on their computers. (CX0711 (Dooley, Dep. at 75-76); (CX0724 (Maire, Dep. at 95-96)).

615. From at least December 2008 through February 2014, AVG was used on the doctors' offices computers. (CX0707 (Bureau, Dep. at 62); CX0705-A (Bradley, Dep. at 82-83)).

Response to Finding No. 615

Respondent has no specific response.

616. From at least May 2010 through February 2014, LabMD did not verify that the AVG software installed on computers provided to physician-clients was working correctly or updating its virus definitions. (CX0705-A (Bradley, Dep. at 84-86)).

Response to Finding No. 616

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Complaint Counsel cannot establish that LabMD did not verify that the AVG software installed on computers provided to physician-clients was working correctly through Mr. Bradley's testimony as cited. Mr. Bradley testified that he did not log in and scan customers' computers. Nowhere did he testify that LabMD never did so. (CX0705-A (Bradley, Dep. at 84-86)).

617. LabMD continued to accept test orders from physician-clients until January 11, 2014. (CX0682 (January 6, 2014 LabMD Letter to Physician's office re Closing)).

Response to Finding No. 617

Respondent has no specific response.

618. Even after it implemented a more capable antivirus application than ClamWin or AVG on employee computers, Trend Micro, LabMD did not install it on all its

equipment, such as physician-clients' computers. (CX0724 (Maire, Dep. at 94-95); CX0727-A (Parr, Dep. at 71)).

Response to Finding No. 618

Respondent objects to this proposed finding of fact to the extent that it suggests that Maire and Parr testified that Trend Micro was a more capable antivirus application than ClamWin or AVG. Neither witness testified to that assertion.

619. Intentionally left blank.

620. Intentionally left blank.

4.3.2.1.3.2 LabMD Did Not Consistently Run Antivirus Scans of Computers Provided To Physician-Clients

621. LabMD did not login and run AVG scans on computers it operated in the offices of physician-clients. (CX0705-A (Bradley, Dep. at 103-106, 118-119)).

Response to Finding No. 621

Respondent objects to this finding of fact because it ignores evidence in the record to the contrary. Mr. Bradley actually testified that he would login and run AVG scans on computers in the physician-client offices when users complained that their computers were not performing adequately. (CX0705-A (Bradley, Dep. at 105-06, 118–19)).

622. LabMD only inspected computers it provided to the offices of physician-clients when the clients complained that the computers were not working, and it never reviewed log reports of the ClamWin antivirus program installed on the computers in physician-client offices. (CX0724 (Maire, Dep. at 48-49, 95-97)).

Response to Finding No. 622

Respondent objects to this finding of fact because it is unsupported by the citations to the record. Mr. Maire did not testify as to whether LabMD ever reviewed log reports of the ClamWin antivirus program installed on physician-client computers. His testimony regarding ClamWin in portions of the record relied upon by Complaint Counsel was limited to whether LabMD employees *updated* ClamWin, not whether it reviewed ClamWin logs. (CX0724 (Maire, Dep. at 48-49, 95-97)).

623. LabMD's sales representatives, rather than its IT employees, generally monitored whether computers installed in the offices of physician clients were working properly. In some instances, after being notified by sales representatives that the computers were not working properly, IT employees found that the computers were infected with viruses and malware. (CX0735 (Kaloustian, IHT at 151-154)).

Response to Finding No. 623

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

624. Intentionally left blank.

625. Intentionally left blank.

4.3.2.1.3.3 LabMD Did Not Consistently Review Antivirus Scans Run on Computers Provided to Physician-Clients

626. From May 2010 through February 2014, the employee responsible for hardware provided to physician-clients did not review the logs of the antivirus program installed on physician-clients' computers. (CX0705-A (Bradley, Dep. at 7-10, 86)).

Response to Finding No. 626

Respondent objects to this proposed finding of fact because it is misleading as it attempts to establish as fact using Bradley's testimony that LabMD did not review the logs of the antivirus program installed on physician-clients' computers. Bradley actually testifies that his primary responsibility was fixing hardware such as printers at LabMD and local customers' offices. Bradley testified that he only reviewed the logs for the LabMD equipment for the LabMD offices. (CX0705-A (Bradley, Dep. at 9, 86)).

627. Intentionally left blank.

4.3.2.1.4 LabMD's Antivirus Applications as Deployed Allowed Viruses To Reach a Server Handling Sensitive Personal Information

628. A number of viruses were observed on LabMD's Mapper server coming from the computers LabMD supplied to doctor's offices. (CX0735 (Kaloustian, IHT at 77-78)).

Response to Finding No. 628

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

629. In 2007 or 2008, a LabMD server was infected with the SQL Slammer Worm; LabMD did not have the tools or experience to determine whether the worm was successful in exporting LabMD's data. (CX0735 (Kaloustian, IHT at 149-50, 263-64)).

Response to Finding No. 629

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing

Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

630. Intentionally left blank.

4.3.2.2 LabMD's Firewall Could Not Reliably Detect Security Risks

631. Ports are associated with particular programs. Therefore, blocking a port means that the program that uses that port cannot send or receive information. (CX0740 (Hill Report) ¶¶ 19, 20, 22, 31).

Response to Finding No. 631

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

632. Traditional firewalls are designed to block specific types of traffic into specific ports, not detect intrusions and attacks. (CX0740 (Hill Report) ¶ 65; Hill, Tr. 95; *see also infra* § 5.8.3 (LabMD Did Not Reasonably Deploy Firewalls) (¶¶ 1075-1082)).

Response to Finding No. 632

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See*

Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

633. An open port is an open door to a computer, even when the program using that port is not running. (CX0740 (Hill Report) ¶ 20).

<u>Response to Finding No. 633</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

634. When a port is blocked or closed, any data that arrives at the network or computer for that port will be discarded. (CX0740 (Hill Report) ¶ 22).

<u>Response to Finding No. 634</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

635. Web servers and browsers typically use ports 80 and 443 for web access. Those ports should be closed when web access is not approved or permitted. (CX0740 (Hill Report) ¶¶ 20, 31(c)).

Response to Finding No. 635

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009)(commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

636. Cypress did not provide firewall or other protections for LabMD's network. (CX0729 (Sandrev, Cypress Designee, Dep. at 54-57, 60-61, 65-68).

Response to Finding No. 636

Respondent has no specific response.

637. LabMD used a ZyWall firewall it obtained from APT from approximately May 2006 until 2010, when it was replaced with a Juniper firewall. (CX0731 (Truett, Dep. at 31, 60-61); CX0710-A (Daugherty, LabMD Designee, Dep. at 177-78); CX0553 (MDS Juniper Proposal)).

Response to Finding No. 637

Respondent has no specific response.

638. LabMD's ZyWall firewalls protected LabMD's inside network – only equipment that was physically inside LabMD's offices and on LabMD's local area network – from the outside public Internet. (CX0731 (Truett, Dep. at 65-66, 73)).

Response to Finding No. 638

Respondent has no specific response.

639. The ZyWall hardware firewall that LabMD used until 2010 had very limited risk assessment capabilities. (CX0740 (Hill Report) ¶ 68(b); *infra* § 5.3.2.2.1 (LabMD Did Not Consistently Review Firewall Logs to Identify Risks) (¶¶ 642-648)).

Response to Finding No. 639

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

640. Intentionally left blank.

641. Intentionally left blank.

4.3.2.2.1 LabMD Did Not Consistently Review Firewall Logs to Identify Risks

642. IT practitioners review firewall logs of network traffic to identify the application and host targets of unauthorized attempts to access the network. (CX0740 (Hill Report) ¶ 65).

Response to Finding No. 642

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

643. The ZyWall firewall LabMD used until 2010 could only store a few days' worth of logging information at a time in its memory (CX0710-A (Daugherty, LabMD Designee, Dep. at 177); CX0731 (Truett, Dep. at 68-69)).

Response to Finding No. 643

Respondent has no specific response.

644. LabMD's firewall logs were erased by overwriting as frequently as every few days. (CX0731 (Truett Dep. at 68-69); CX0733 (Boyle, IHT at 86-88); (CX0710-A (Daugherty 30(b)(6) Dep. at 176-177)).

Response to Finding No. 644

Respondent has no specific response.

645. The Zywall firewall had fairly limited logging features embedded in the device, and logged only connectivity information of traffic going in and out of the equipment. For example, if someone visited a web page, there would be a log entry of the computer that accessed the web page and the host IP address of the website embedded in the device. (CX0731 (Truett, Dep. at 68)).

Response to Finding No. 645

Respondent has no specific response.

646. LabMD did not systematically review the firewall's limited logs to detect attempted unauthorized network access. (*Infra* ¶¶ 647-648).

Response to Finding No. 646

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

647. APT did not review any LabMD firewall logs unless it was trying to troubleshoot a problem, such as with Internet speed or connectivity. (CX0731 (Truett, Dep. at 69)).

Response to Finding No. 647

Respondent has no specific response.

648. Between March 2004 and April 2009, LabMD employees did not review network activity logs unless there was a problem, such as the Internet being down. (CX0717

(Howard, Dep. at 99); CX0711 (Dooley, Dep. at 51-52); CX0735 (Kaloustian, IHT at 107-08)).

<u>Response to Finding No. 648</u>

Respondent has no specific response.

649. Intentionally left blank.

650. Intentionally left blank.

4.3.2.2.2 LabMD Did Not Consistently Monitor Traffic Through Its Firewall

651. IT practitioners use traffic monitoring to, for example, determine if sensitive consumer information is being exported from their networks without authorization. (CX0740 (Hill Report) ¶ 68(b)).

<u>Response to Finding No. 651</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

652. The Zywall firewall had no traffic monitoring features. (CX0731 (Truett, Dep. at 67)).

<u>Response to Finding No. 652</u>

Respondent has no specific response.

653. As of October 2006, LabMD's firewalls did not have the capability of inspecting packets, and through April 2009 LabMD did not have any tools or practices to inspect the content of Internet traffic into and out of its network. (CX0735 (Kaloustian, IHT at 102, 270)).

<u>Response to Finding No. 653</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.")

654. Between March 2004 and April 2009, LabMD did not monitor traffic on its network. (CX0717 (Howard, Dep. at 57, 139); CX0735 (Kaloustian, IHT at 107-08)).

<u>Response to Finding No. 654</u>

Respondent objects to this finding of fact because it is unsupported by the citation to the record. The cited portions of the record do not refer to a time period between "March 2004 and April 2009."

655. From 2004 through at least March 2007, LabMD did not capture electronically the data that was outbound from the network or where the data was going. (CX0717 (Howard, Dep. at 138)).

<u>Response to Finding No. 655</u>

Respondent objects to this finding of fact because it is unsupported by the citation to the record. The cited portions of the record do not refer to a time period from "2004 through at least March 2007."

656. Even where a gateway firewall is appropriately deployed, a layered data security strategy instructs that a second layer of security may be appropriate. (CX0740 (Hill Report) ¶ 29(b)). The firewall at the gateway may be misconfigured, for example, and not discard all unauthorized traffic. (CX0740 (Hill Report) ¶ 29(b)). To mitigate this danger, software firewalls can be deployed at workstations and servers to further filter traffic. (CX0740 (Hill Report) ¶ 29(b)).

<u>Response to Finding No. 656</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

657. However, LabMD did not log activity on employee computers. (CX0717 (Howard, Dep. at 98-99)).

Response to Finding No. 657

Respondent has no specific response.

658. Intentionally left blank.

659. Intentionally left blank.

4.3.2.3 LabMD's Manual Inspections Could Not Reliably Detect Security Risks

660. Even when conducted on a regular basis, manual computer inspections are error-prone and can never be exhaustive because vulnerabilities and risks can exist anywhere in a computer, and human beings cannot inspect every one of those places. There are configurations in multiple places, including configuration of the firewall, so there are many aspects of the computer that would need to be inspected, including antivirus logs and any logs that the operating system may generate. Because of the multiplicity of items that need to be checked, it is virtually impossible for manual inspections to be effective as a risk assessment tool. (CX0740 (Hill Report) ¶ 68(c); Hill, Tr. 151-52).

Response to Finding No. 660

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

661. Furthermore, malicious software may, in some instances, mask its presence to avoid detection during a manual inspection, such as by altering the task manager application in Windows to prevent the malicious software's process from being displayed. (CX0740 (Hill Report) ¶ 68(c)).

Response to Finding No. 661

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

662. IT practitioners should not rely on manual inspections and should also use automated mechanisms, such as IDS, file integrity monitoring, and penetration testing to assess risks and vulnerabilities on the network. (CX0740 (Hill Report) ¶ 68(c)).

Response to Finding No. 662

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

663. Between May 2010 and February 2014, LabMD IT employees were to manually verify certain aspects of employee computers set out in Exhibit CX0169 (IT Tools/Checks-handwritten-Administrators Old Computer). (CX0705-A (Bradley, Dep. at 77-78)).

Response to Finding No. 663

Respondent objects to this proposed finding of fact because it is misleading as it ignores evidence in the record to the contrary. IT Manager Bob Hyer (CX0704 (Boyle, Dep. at 12)), who was employed at LabMD from June 2009 to March 2012, (CX0719, (Hyer, Dep. at 143)), testified that the checklist referred to the scans which made the manual review unnecessary. (CX0719, (Hyer, Dep. at 99)). Furthermore, the cited portions of the record do not refer to the time period “May 2010 and February 2014.”

664. Some of the verifications in Exhibit CX0169 could have been performed automatically rather than manually. (CX0705-A (Bradley, Dep. at 80-82)).

Response to Finding No. 664

Respondent has no specific response.

665. Automating these security verifications would require purchasing software rather than using "shareware." (CX0705-A (Bradley, Dep. at 79-81)).

Response to Finding No. 665

Respondent has no specific response.

666. Intentionally left blank.

667. Intentionally left blank.

4.3.2.3.1 LabMD IT Employees Performed Manual Inspections Only on Request When Employee Workstations Malfunctioned

668. From March 2004 to at least October 2009, LabMD did not inspect employee desktops for security issues on a regular basis. (CX0717 (Howard, Dep. at 102-03); CX0711 (Dooley, Dep. at 64-65, 122-23); CX0735 (Kaloustian, IHT at 177); CX0730 (Simmons, Dep. at 104, 143-45); CX0734 (Simmons, IHT at 78-79).

Response to Finding No. 668

Respondent has no specific response.

669. Rather, LabMD IT employees inspected employee workstations only if the employee requested it because the computer was not functioning properly. (CX0730 (Simmons, Dep. at 104, 144-45); CX0734 (Simmons, IHT at 78-79); CX0707 (Bureau, Dep. at 51, 89-90)).

Response to Finding No. 669

Respondent has no specific response.

670. When so-called "daily walkarounds" were allegedly instituted in May 2008, *infra* ¶ 680, through at least April of 2010 they consisted of an IT employee visiting each section of the office to query end users if they had any issues with their computers. (CX0724 (Maire, Dep. at 46); CX0707 (Bureau, Dep. at 50-51)).

Response to Finding No. 670

Respondent has no specific response.

671. LabMD's manual inspections focused on quickly fixing performance problems on computers used by employees. (CX0734 (Simmons IHT at 79-84)).

Response to Finding No. 671

Respondent objects to this finding of fact because it is unsupported by the citations to the record. Ms. Simmons does not testify that her inspections were focused on "quickly fixing performance problems on computers used by employees." In fact, Ms. Simmons outlines a lengthy series of steps she would take in order to resolve issues a user might be having. She stated that she would "work with the computer until it was fixed." (CX0734 (Simmons, IHT at 81)). Manual inspections of employee computers could take as long as several hours. (CX0705-A (Bradley, Dep. at 77)).

672. Manual inspections of employee computers took place during regular business hours, when employees were using the computers to do their work. (CX0734 (Simmons, IHT at 83-84); CX0705-A (Bradley, Dep. at 77); CX0724 (Maire, Dep. at 47); CX0719 (Hyer, Dep. at 96)).

Response to Finding No. 672

Respondent has no specific response.

673. LabMD's IT employees performed manual inspections of employee computers by sitting at the workstations and working with the computers, so that employees could not use the computers while they were being manually inspected. (CX0705-A (Bradley, Dep. at 77); CX0734 (Simmons, IHT at 84)).

Response to Finding No. 673

Respondent has no specific response.

674. Manual inspections of employee computers could take as long as several hours. (CX0705-A (Bradley Dep. at 77)).

Response to Finding No. 674

Respondent has no specific response.

675. One IT employee testified that from mid-2007 through June 2008, he would inspect computers to make sure the appropriate programs were installed and uninstall the games that were on the computers. Other than Windows games, the employee

testified that he did not see applications on the LabMD computers he needed to remove. (CX0724 (Maire, Dep. at 52-53)).

Response to Finding No. 675

Respondent has no specific response.

676. However, other IT employees testified that they did not proactively review employee workstations on a regular basis. (CX0711 (Dooley, Dep. at 64-65, 122-23); CX0735 (Kaloustian, IHT at 177); CX0730 (Simmons, Dep. at 104, 144-45); CX0734 (Simmons, IHT at 78-79); CX0707 (Bureau, Dep. at 50-52, 89-90); *see also* CX0719 (Hyer, Dep. at 95) (August 2009-September 2011)).

Response to Finding No. 676

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited portions of Mr. Hyer's testimony not only fail to support Complaint Counsel's proposed finding of fact, it directly contradicts it. Mr. Hyer actually testified as follows:

> Q. Okay. I know earlier we talked about some review of desktop computers and I want to turn back to that. Just to make sure I understood your testimony earlier, did you manually inspect computers at LabMD?
>
> A. Not as a formal practice, but when they was on any one of the computers I would poke around to see if there was anything I should know. Most of the time, there was none.
>
> Q. Okay. So when you say there's, in your words, anything you should know, what types of things were you looking for?
>
> A. Anything out of the ordinary which was within standard configuration and -- and policies.

> Q. Give me a couple examples.
>
> A. Screen savers.
>
> Q. Are there – were there any particular security-related things you were looking for?
>
> A. No. We had the security locked down pretty tight.
>
> Q. How frequently did you do these manual inspections of computers?
>
> A. Just as part of my daily process.
>
> Q. And you can correct me if I'm wrong, but I think you -- I think I'm remembering now you said earlier it wouldn't have been -- would not have been more than once a week on average?
>
> A. Yeah, yeah, just...
>
> Q. Did that frequency change materially during your tenure at LabMD?
>
> A. No.

(CX0719 (Hyer, Dep. at 95-96)).

677. In the course of providing requested maintenance, an IT employee might look at the installed applications on the computer's Control Panel to see what employees had installed, but it was not a regular event and did not occur on randomly selected computers. (CX0707 (Bureau, Dep. at 95-96)).

<u>Response to Finding No. 677</u>

Respondent has no specific response.

678. Intentionally left blank.

679. Intentionally left blank.

4.3.2.3.2 LabMD Did Not Provide Guidance For Manual Inspections of Employee Computers Until 2010, And Thereafter Employees Did Not Always Follow The Guidance

680. According to LabMD, in May 2008, it designated an employee as the IT Department desktop specialist to manually conduct "daily walkaround" desktop

computer system reviews to confirm security status, functioning, verify absence of downloaded software or files, update software, address error messages, issues, and IT requests from managers or employees, address interface issues with clinical equipment and systems, and take steps to remediate data security problems, if necessary. (CX0445 (LabMD Access Letter Response by Phillipa Ellis) at 2).

Response to Finding No. 680

Respondent has no specific response.

681. LabMD allegedly created a checklist for employees to use in the daily walkaround. (CX0482 (IT Dept Walkaround Checklist)).

Response to Finding No. 681

Respondent has no specific response.

682. The Walkaround Checklist, Exhibit CX0482, was not in use from October 2006 through August 2009. (CX0730 (Simmons, Dep. at 143)).

Response to Finding No. 682

Respondent objects to this finding of fact because it is unsupported by the citation to the record. Ms. Simmons did not testify that the checklist was not in use from October 2006 through 2009. Without specifying a date as to when she was referring, Ms. Simmons testified only that she was "not sure if the checklist was ever followed for walk-around inspections." (CX0730 (Simmons, Dep. at 143)).

683. During his tenure from June 2009 to September 2011, Mr. Hyer did not follow a checklist when he manually inspected LabMD employee computers. (CX0719 (Hyer, Dep. at 98)).

Response to Finding No. 683

Respondent has no specific response.

684. No IT Department employee other than Mr. Hyer manually inspected LabMD computers between 2009 and 2012. (CX0719 (Hyer, Dep. at 99)).

Response to Finding No. 684

Respondent has no specific response.

685. Mr. Hyer kept no records of his manual inspections. (CX0719 (Hyer, Dep. at 99)).

Response to Finding No. 685

Respondent has no specific response.

686. Intentionally left blank.

4.3.2.3.3 LabMD Did Not Inspect Computers Provided To Sales Representatives

687. LabMD did not inspect the laptop computers of its sales representatives or ask about warnings, errors, or application messages to laptop users. (CX0718 (Hudson, Dep. at 184); CX0722 (Knox, Dep. at 58)).

Response to Finding No. 687

Respondent objects to this finding of fact as it is unsupported by the citation to the record. Complaint Counsel cannot not establish that LabMD did not inspect the laptop computers of its sales representatives or ask about warnings, errors, or application messages to laptop users with the testimony cited above. Hudson testified that LabMD's IT staff did not ask **him personally** about warnings, errors, or application messages; and he was never asked about inspections of his laptop. (CX0718 (Hudson, Dep. at 184)). Knox testified he doesn't remember being asked to allow LabMD to inspect **his** computer, nor does he remember ever seeing or being asked about warnings, errors, or application messages. (CX0722 (Knox, Dep. at 58)).

688. Intentionally left blank.

4.3.2.3.4 LabMD Did Not Inspect Computers Provided To Physician-Clients Except When It Received Complaints

689. From at least March 2006 through August 2009, LabMD did not conduct regular security inspections of the computers it provided to physician-clients, and performed inspections and maintenance only in response to complaints from the physician-clients. (CX0711 (Dooley, Dep. at 68-69) (March 2006 through December 2006); CX0724 (Maire, Dep. at 48-49) (June 2007 through June 2008); CX0734 (Simmons, IHT at 85-86) (October 2006 through August 2009)).

Response to Finding No. 689

Respondent has no specific response.

690. Intentionally left blank.

4.3.2.3.5 LabMD's Manual Inspections Did Not Detect The LimeWire Application Installed On The Computer Used By LabMD's Billing Manager

691. LimeWire was installed on the computer used by LabMD's billing manager between approximately 2005 and 2008. (*Infra* § 8.1.3.1 (After Being Notified About Availability of 1718 File, LabMD Discovered LimeWire on a Billing Computer) (¶¶ 1399-1406).

Response to Finding No. 691

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

692. The LimeWire application installed on the computer used by LabMD's billing manager was not needed for business purposes. (Ans. ¶ 20).

Response to Finding No. 692

Respondent has no specific response.

693. If LabMD had implemented a policy to identify and remove unauthorized software, as it claims, it would have detected the LimeWire application on the billing manager's computer. (CX0740 (Hill Report) ¶ 61(b)).

Response to Finding No. 693

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

694. The only IT employee who testified to regularly and proactively inspecting computers from mid-2007 through June 2008 to make sure the appropriate programs were installed and uninstall unauthorized programs did not see applications on the LabMD computers he needed to remove other than Windows games, although LimeWire was installed on the billing manager's computer during this time frame. (CX0724 (Maire, Dep. at 52-53); *Infra* § 8.1.3.1 (After Being Notified About Availability of 1718 File, LabMD Discovered LimeWire on a Billing Computer) (¶¶ 1399-1406)).

<u>Response to Finding No. 694</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. Mr. Maire did not testify that he was the "only IT employee who testified to regularly and proactively inspected computers" during this period. Maire was never asked about LimeWire.

Respondent further objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

695. LimeWire was not detected until after LabMD was notified that the 1718 File was available on a P2P network. (*Infra* § 8.1.3.1 (After Being Notified About Availability of 1718 File, LabMD Discovered LimeWire on a Billing Computer) (¶¶ 1399-1406)).

Response to Finding No. 695

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

696. Even after LabMD knew LimeWire had been installed on one of its computers, LabMD IT employees' manual inspections of LabMD desktop computers would not necessarily have detected the installation of a peer-to-peer program. (CX0719 (Hyer, Dep. at 99)).

Response to Finding No. 696

Respondent has no specific response.

697. Intentionally left blank.

698. Intentionally left blank.

4.3.3 LabMD Did Not Implement Automated Scanning Tools

4.3.3.1 LabMD Did Not Implement An Intrusion Detection System ("IDS") or Intrusion Protection System ("IPS")

699. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using automated mechanisms, such as an IDS. (CX0740 (Hill Report) ¶ 69).

Response to Finding No. 699

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

700. An IDS acts like a sensor to detect malicious activity on a system; it can be used to detect attacks and alert the IT staff that firewall settings should be reconfigured. (CX0740 (Hill Report) ¶ 65; Hill, Tr. 99).

Response to Finding No. 700

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

701. Without an IDS, a company cannot determine if it has been subjected to the types of threats that an IDS would identify. For example, a firewall does not have the same ability as an IDS to capture large amounts of traffic to perform analysis on that traffic and alert IT of possible threats and suspicious activities. (CX0740 (Hill Report) ¶ 65; Hill, Tr. 149; *supra* § 5.3.1.3 (Many Tools Are Available to Assess and Remediate Risk) (¶¶ 514-521)).

Response to Finding No. 701

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

702. LabMD did not implement an IDS or an IPS. (CX0731 (Truett, Dep. at 122); CX0717 (Howard, Dep. at 58, 140-41); CX0711 (Dooley, Dep. at 108-09); CX0735 (Kaloustian, IHT at 92); CX0719 (Hyer, Dep. at 123-24, 126); CX0705-A (Bradley, Dep. at 48)).

<u>Response to Finding No. 702</u>

Respondent objects to this proposed finding of fact because it is not specific to time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

703. Intentionally left blank.

704. Intentionally left blank.

4.3.3.2 LabMD Did Not Implement File Integrity Monitoring

705. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using automated mechanisms, such as file integrity monitoring. (CX0740 (Hill Report) ¶ 69).

<u>Response to Finding No. 705</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

706. File integrity monitoring can identify changes in critical files that may indicate malware has been installed on the network, but does not identify or remove the malware. (CX0740 (Hill Report) ¶¶ 65, 104(h)).

Response to Finding No. 706

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

707. File integrity monitoring tools are the types of mechanisms that IT practitioners used regularly through the Relevant Time Period. (CX0740 (Hill Report) ¶ 104(h)).

Response to Finding No. 707

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

708. File integrity monitoring is more efficient and significantly more effective than manual inspections, because manual inspections cannot be exhaustive and people cannot manually inspect every place in a computer where vulnerabilities and risks might exist. (CX0737 (Hill Rebuttal Report) ¶ 28).

Response to Finding No. 708

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

709. File integrity monitoring could have detected the LimeWire file-sharing application on the computer used by LabMD's billing manager. (CX0740 (Hill Report) ¶ 105(b)).

Response to Finding No. 709

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

710. LabMD did not implement file integrity monitoring. (CX0735 (Kaloustian, IHT at 92-93); CX0734 (Simmons, IHT at 68-69); CX0705-A (Bradley, Dep. at 46-47)).

Response to Finding No. 710

Respondent has no specific response.

711. From October 2006 to April 2009, LabMD did not have any tools or practices in place capable of detecting the installation of a P2P application. (CX0735 (Kaloustian, IHT at 269-70); CX0734 (Simmons, IHT at 160)).

Response to Finding No. 711

Respondent has no specific response.

712. Prior to May 2008, LabMD did not detect the installation or use of LimeWire on any LabMD computer. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 9, Adms. 43-44).

Response to Finding No. 712

Respondent has no specific response.

713. Intentionally left blank.

714. Intentionally left blank.

4.3.4 LabMD Did Not Use Penetration Testing Before 2010

715. Penetration tests remotely audit and analyze the system and provide a "hacker's eye view" of the system to discover its security vulnerabilities and weaknesses to possible hacker penetration or attack. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 2; CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002) at 24-25).

Response to Finding No. 715

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

716. Penetration tests have been available to IT practitioners since at least 1997. (CX0740 (Hill Report) ¶ 71).

Response to Finding No. 716

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

717. LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using automated mechanisms, such as penetration testing. (CX0740 (Hill Report) ¶ 69).

Response to Finding No. 717

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

718. A penetration test of all IP addresses on the network would have identified vulnerabilities such as outdated software, security patches that had not been applied, administrative accounts with default settings, and all open ports within the network and all computers that accepted connection requests. (CX0740 (Hill Report) ¶ 70).

Response to Finding No. 718

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

719. IT practitioners use this information to identify risks early and address these vulnerabilities. (CX0740 (Hill Report) ¶¶ 70, 76).

Response to Finding No. 719

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

720. Many penetration testing tools were available to LabMD at no cost. (*Infra* § 6.3.4.1 (Penetration Testing Tools Were Readily Available To LabMD Years Before It Began Penetration Testing) (¶¶ 1140-1142)).

Response to Finding No. 720

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

Respondent further objects to this proposed finding of fact because it is not specific to time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

721. LabMD did not conduct any penetration tests on its network until May 2010. (JX0001-A (Joint Stips. of Fact, Law, and Auth.) at 4; CX0735 (Kaloustian, IHT at 92, 281-82); CX0719 (Hyer, Dep. at 164, 175-76); CX 0734 (Simmons, IHT at 67-68); CX0731 (Truett, Dep. at 119-123; CX0724 (Maire, Dep. at 92); CX0717 (Howard, Dep. at 56-58); CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 5; CX0052 (Final Page of ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty and H. Davidson)).

Response to Finding No. 721

Respondent has no specific response.

722. APT did not use any tools to assess risks and vulnerabilities on LabMD's network, did not assess potential risks and vulnerabilities associated with LabMD's network, and did not consult any resources like SANS, CERT, or CBE to identify risks to LabMD's network. (CX0731 (Truett, Dep. at 119-21)).

Response to Finding No. 722

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record to the contrary by stating that "LabMD did not assess potential risks and vulnerabilities associated with its network." Truett actually testifies that as per his contract with LabMD he provided industry standards and best practices based upon what other medical practices and medical organizations did. He understood the threats and risk mitigation and the precautions to take against them. (CX0731 (Truett, Dep. at 44-46)).

723. From October 2006 through August 2009 LabMD's IT employees did not have any tools to perform automated scans on employee computers or the network for unauthorized programs or outbound traffic. (CX0734 (Simmons, IHT at 107-08)).

Response to Finding No. 723

Respondent objects to this proposed finding of fact because it is an attempt to mislead the Court despite clear evidence in the record to the contrary. Clam Win ran scans on a schedule. It also ran updates on a schedule to check for virus signatures in real time. (CX0711 (Dooley, Dep. at 75, 88); (CX0724 (Maire, Dep. at 95-96); (CX0734 (Simmons, IHT at 88-90)). LabMD IT employee Dooley started with LabMD in November of 2004 and ended his employment with LabMD in December 2006. (CX0711 (Dooley, Dep. at 12-13)). LabMD IT employee Maire started with LabMD in mid 2007 and left in mid 2008. (CX0724 (Maire, Dep. at 10)). LabMD IT employee Simmons started with LabMD in October 2006 and left in August 2009. (RX 508 (Simmons, Dep. at 10)).

724. ProviDyn began conducting scans for LabMD in May or June 2010. (CX0719 (Hyer, Dep. at 107); CX0042 (Email H. Davidson to M. Daugherty Subject RE: ProviDyn Follow Up, attaching LabMD External Vulnerability Scan.pdf, Auth. To Perform External Network Scan.doc); CX0710-A (Daugherty, LabMD Designee, Dep. at 150-51)).

Response to Finding No. 724

Respondent has no specific response.

725. LabMD did not conduct on its own any penetration tests equivalent to the ones that ProviDyn conducted. (CX0719 (Hyer, Dep. at 164)).

Response to Finding No. 725

Respondent has no specific response.

726. Even when LabMD did penetration testing in 2010, the tests were limited to external facing servers and did not test employee workstations and computers inside LabMD's network. (CX0719 (Hyer, Dep. at 105); CX0042 (Email H. Davidson to M. Daugherty, Subject RE: ProviDyn Follow Up, attaching LabMD External Vulnerability Scan.pdf, Auth. To Perform External Network Scan.doc) at 7; CX0044

(ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4-5; CX0048 (ProviDyn Invoice May 25, 2010)).

Response to Finding No. 726

Respondent has no specific response.

727. Intentionally left blank.

728. Intentionally left blank.

4.3.4.1 Penetration Testing Performed in 2010 Revealed Vulnerabilities on LabMD's Servers

729. On May 21, 2010, ProviDyn analyzed penetration tests on nine LabMD servers. (CX0051 (LabMD ProviDyn May 2010 Penetration Test Agreement) at 4; CX0066 (May 2010 Penetration Test of Firewall); CX0067 (May 2010 Penetration Test of LabNet Server); CX0068 (May 2010 Penetration Test of Mail Server); CX0069 (May 2010 Penetration Test of Router); CX0070 (May 2010 ProviDyn Network Security Scan-Mapper); CX0071 (May 2010 Penetration Test of Demographics Server); CX0072 (May 2010 Penetration Test of Specialty VPN Server); CX0073 (May 2010 Penetration Test of Printer Server); CX0074 (May 2010 Penetration Test of LabCorp VPN Server); CX0048 (ProviDyn Invoice May 25, 2010)).

Response to Finding No. 729

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

730. Included among the nine servers were two servers named "Specialty VPN" and "LabCorp VPN" located respectively at IP addresses 64.190.124.9 and 64.190.124.14 on LabMD's network. (CX0051 (LabMD ProviDyn May 2010 Penetration Test Agreement) at 4).

Response to Finding No. 730

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was

contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

731. The Specialty VPN and LabCorp VPN servers connected to two outside "reference" laboratories, namely, Specialty Labs and LabCorp. (CX0443 (Feb. 24, 2010 Letter from P. Ellis to A. Sheer) at 5-7; CX0034 (LabMD-Powers Ferry Road Location) at 2; CX0041 (LabMD-Powers Ferry Road Location 2011)).

Response to Finding No. 731

Respondent has no specific response.

732. Each of the two reference laboratories, rather than LabMD, controlled the security measures in place on its server. (CX0443 (Feb. 24, 2010 Letter from P. Ellis to A. Sheer) at 5-7; CX0034 (LabMD-Powers Ferry Road Location) at 2; CX0041 (LabMD-Powers Ferry Road Location 2011)).

Response to Finding No. 732

Respondent has no specific response.

733. The security measures in place on the seven other servers were controlled by LabMD. (*Supra* §§ 4.7.1 (LabMD Internally Managed Its Network) (¶ 173), 4.7.2 (LabMD Used Outside Contractors Only for Limited Tasks) *et seq.* (¶¶ 175-190); CX0735 (Kaloustian, IHT at 98-99)).

Response to Finding No. 733

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

Respondent further objects to this proposed finding of fact to the extent it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

734. On July 18, 2010, ProviDyn analyzed penetration tests on three LabMD servers, including Mapper. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper)).

Response to Finding No. 734

Respondent has no specific response.

735. On September 3, 2010, ProviDyn again analyzed penetration tests on the nine LabMD servers it analyzed in May. (CX0057 (September 2010 Penetration Test of Firewall); CX0058 (September 2010 Penetration Test of LabNet Server); CX0059 (September 2010 Penetration Test of Mail Server); CX0060 (September 2010 Penetration Test of Router); CX0061 (September 2010 ProviDyn Network Security Scan-Mapper); CX0062 (September 2010 Penetration Test of Demographics Server); CX0063 (September 2010 Penetration Test of Specialty VPN Server); CX0064 (September 2010 Penetration Test of Printer Server); and CX0065 (September 2010 Penetration Test of LabCorp VPN Server)).

Response to Finding No. 735

Respondent has no specific response.

736. ProviDyn ranked the "security posture" of each server according to the number and severity of the vulnerabilities discovered by penetration testing, using a five grade scale: Poor, Fair, Average, Very Good, and Excellent. (CX0072 (May 2010 Penetration Test of Specialty VPN Server) ("Excellent"); CX0066 (May 2010 Penetration Test of Firewall) ("Very Good"); CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) ("Average"); CX0059 (September 2010 Penetration Test of Mail Server) ("Fair"); CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) ("Poor")).

Response to Finding No. 736

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was

contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

737. In its penetration test analyses, ProviDyn used a five level classification system: Urgent Risk (5), Critical Risk (4), High Risk (3), Medium Risk (2), and Low Risk (1) based on international and recognized industry standards including the PCI Security Standard and the Common Vulnerability Scoring System (CVSS) established by the National Institute of Standards (NIST). (CX0740 (Hill Report) ¶ 73 & n.24; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 737

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

738. Level 5 (Urgent Risk) Vulnerabilities allow hackers to compromise the entire host. Level 5 includes vulnerabilities provide remote hackers with full file-system read and write capabilities, remote execution of commands as an administrative user. (CX0740 (Hill Report) ¶ 73 & n.24; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 738

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

739. Level 4 (Critical Risk) vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as level 4 vulnerabilities. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 739

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

740. Level 3 (High Risk) vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerability could result in potential misuse of the host by intruders. Examples of level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying). (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 740

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

741. Level 2 (Medium Risk) vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 741

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

742. Level 1 (Low Risk) vulnerabilities are informational, such as open ports. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

Response to Finding No. 742

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

743. The penetration tests conducted in 2010 identified a number of well-known and significant risks and vulnerabilities on LabMD's network, including some that had been known to IT practitioners for years. (CX0740 (Hill Report) ¶ 72).

Response to Finding No. 743

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

744. Intentionally left blank.

745. Intentionally left blank.

4.3.4.2 Penetration Testing Performed in 2010 Indicated That The Security Posture of Several LabMD Servers That Handled Sensitive Information Was Poor

746. On May 21, 2010, ProviDyn conducted a penetration test on LabMD's Mapper, LabNet, Mail, and Demographics servers. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 1, 14; CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4); CX0067 (May 2010 Penetration Test of LabNet Server); CX0068 (May 2010 Penetration Test of Mail Server); CX0071 (May 2010 Penetration Test of Demographics Server)).

Response to Finding No. 746

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

747. In May 2010, ProviDyn rated the security posture each of these servers as "Poor." (CX0067 (May 2010 Penetration Test of LabNet Server) at 1; CX0068 (May 2010 Penetration Test of Mail Server) at 1; CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 1; CX0071 (May 2010 Penetration Test of Demographics Server) at 1).

Response to Finding No. 747

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

748. In September 2010, ProviDyn continued to rate the security posture of the LabNet server "Poor," and the Mapper server as "Average." (CX0058 (Providyn Network Security Scan-LabNet) at 1; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 1).

Response to Finding No. 748

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

749. By contrast, the May 2010 ProviDyn penetration tests of the reference laboratory servers found that the overall security posture of the Specialty VPN server was "Excellent" and that the overall security posture of the LabCorp VPN server was "Very Good." (CX0072 (May 2010 Penetration Test of the Specialty VPN Server) at 1; CX0074 (May 2010 Penetration Test of the LabCorp VPN Server) at 1).

Response to Finding No. 749

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

750. Intentionally left blank.

751. Intentionally left blank.

4.3.4.3 The Mapper Server Had Several High Risk Vulnerabilities

752. LabMD used Mapper to receive Personal Information about hundreds of thousands of consumers from physician-clients. (*Supra* §§ 4.6.2.1 (Consumers' Personal Information Transferred to LabMD Electronically) (¶¶ 84-90), 4.7.3.2.1 (Mapper Server) (¶¶ 220-223)).

Response to Finding No. 752

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

753. In May 2010, ProviDyn conducted a penetration test of the Mapper server and concluded that Mapper's security posture was "Poor (100%)." (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 1).

Response to Finding No. 753

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

754. The May 2010 penetration test identified 32 vulnerabilities on Mapper, including one Urgent, one Critical, two High, and three Medium risk vulnerabilities. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 7-8).

Response to Finding No. 754

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

755. In July 2010, ProviDyn conducted a penetration test of the Mapper server and concluded that the Mapper server's security posture was "Poor." (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 1; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 1).

Response to Finding No. 755

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

756. In September 2010, ProviDyn conducted a penetration test of the Mapper server and concluded that the Mapper server's security posture was "average." **(**CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 1).

Response to Finding No. 756

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

4.3.4.3.1 The Mapper Server Had Several High Risk Vulnerabilities Related to an FTP Program Running On It

757. ProviDyn's May, July, and September 2010 penetration tests of the Mapper server found that port 21 was open and that it provided access to a Microsoft FTP program running on Mapper. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 5, 7; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 5, 7; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 5, 7).

Response to Finding No. 757

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

758. Intentionally left blank.

4.3.4.3.1.1 The Mapper Server Had an Anonymous FTP Vulnerability that Could Allow Export of All Data on the Server

759. Among the 32 vulnerabilities it identified on Mapper, ProviDyn's May 2010 penetration test identified a Level 5 anonymous FTP problem, called "Anonymous FTP Writeable root Directory." (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 759

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

760. The Anonymous FTP Writeable root Directory vulnerability may allow an attacker to write on the root directory of the server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; Hill, Tr. 159-60).

Response to Finding No. 760

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

761. To write is to place files from a remote machine onto one of LabMD's servers. This makes changes to the hard disks that are stored within LabMD's network. (Hill, Tr. 113).

Response to Finding No. 761

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

762. This vulnerability would allow an attacker to control and reconfigure the server and turn the server into a software distribution point that would allow the attacker to distribute any data that is on the server to anywhere on the Internet. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; Hill, Tr. 159-60).

Response to Finding No. 762

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

763. ProviDyn identified the Anonymous FTP Writeable root Directory vulnerability by running the Nessus application on Mapper. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 763

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

764. ProviDyn found the Anonymous FTP Writeable root Directory vulnerability was still present on Mapper during the July 2010 penetration test. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 764

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

765. ProviDyn identified publicly available information about the Anonymous FTP Writeable root Directory vulnerability, including CVE and US-CERT references. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 765

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

766. The May 2010 ProviDyn test noted that the CVE identifier for the Anonymous FTP Writeable root Directory vulnerability is CVE 1999-0527. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 766

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

767. The CVSS severity rating included in the May and July 2010 ProviDyn test reports classified the vulnerability as easy to exploit, leading to complete compromise of the confidentiality, integrity, and availability of the Mapper server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 767

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

768. Information about the Anonymous FTP Writeable root Directory vulnerability was first reported by the security community on July 14, 1993 and was included in the CVE in 1999. CX0740 (Expert Report of Raquel Hill) at 63 (citing NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId =CVE-1999-0527)).

Response to Finding No. 768

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

769. A solution to this vulnerability has been known for years: restrict write access to the server's root directory to only authorized users who have been authenticated by their unique credentials. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18 (both referencing 1993 CERT advisory at http://www.cert.org/advisories/CA-1993-10.html)).

Response to Finding No. 769

Respondent objects to this proposed finding of fact because it is not specific to time frame as required by the post trial briefing order. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 4 (July 16, 2015) (mandating that "[i]n addition such proposed findings related to reasonableness shall, without limitation, consider, address, and/or refer to data security requirements and practices prevailing during the relevant time period in this case.").

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

770. ProviDyn identified a solution for the Anonymous FTP Writeable root Directory vulnerability: "restrict write access to the root directory." (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 19; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

<u>Response to Finding No. 770</u>

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

771. The anonymous FTP problem posed an urgent risk to an application that LabMD used to transmit large amounts of Personal Information that could result in a high level of harm. (CX0740 (Hill Report) ¶ 76).

<u>Response to Finding No. 771</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

772. Intentionally left blank.

773. Intentionally left blank.

4.3.4.3.1.2 The Mapper Server Had an FTP Vulnerability that Could Be Exploited to Use the Server To Host Illegal Data

774. The July 2010 ProviDyn penetration test of Mapper detected 30 vulnerabilities, including a Level 4 FTP Critical Risk vulnerability, called "FTP Writeable Directories," that was not present during the May 2010 penetration test. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 1, 8, 18-19, 34).

Response to Finding No. 774

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

775. The FTP Writeable Directories vulnerability means that several directories were marked as being "world-writeable." Thus, an attacker could use the FTP server to host arbitrary data, including potentially illegal content, such as movies, music, and software. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18; Hill, Tr. 159).

Response to Finding No. 775

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

776. The CVSS severity rating included in the July 2010 ProviDyn test report classified the vulnerability as easy to exploit, leading to partial compromise of the integrity and availability of the Mapper server. **(**CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 776

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

777. The CVE alert for this vulnerability, CVE-1999-0527, was released in 1999. **(**CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 777

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

778. The solution to this vulnerability has been known for years: set up the directories so that they are not world-writeable from outside LabMD's network. **(**CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 778

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

779. Intentionally left blank.

780. Intentionally left blank.

4.3.4.3.1.3 The Mapper Server Had a Vulnerability that Could Be Exploited To Access Any Files Available On Mapper

781. ProviDyn detected a Level 2 vulnerability of "Anonymous FTP Enabled" on Mapper in May 2010. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21).

Response to Finding No. 781

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

782. The Anonymous FTP Enabled vulnerability means that the FTP application on Mapper was set up so that any remote user could connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0740 (Hill Report) ¶ 76).

Response to Finding No. 782

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

783. ProviDyn found the Anonymous FTP Enabled vulnerability was still present on Mapper during the July 2010 penetration test, when it was classified as a Level 3 vulnerability. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 783

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

784. ProviDyn identified this vulnerability by running the Nessus application on Mapper. (C0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19)).

Response to Finding No. 784

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

785. In the "Additional References" section, ProviDyn provided publicly available information about the Anonymous FTP Enabled vulnerability, including the CVE reference. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 785

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

786. The May and July 2010 ProviDyn tests noted that the CVE identifier for this vulnerability is CVE 1999-0497, indicating that the vulnerability was first added to the CVE in 1999. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 786

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

787. The CVSS severity rating included in the May and July 2010 ProviDyn test reports classified the vulnerability as easy to exploit, leading to partial compromise of the confidentiality of information on the Mapper server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 787

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

788. A solution to this vulnerability had been known for years: disable anonymous log-ins and periodically review files to ensure sensitive content is not available. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 788

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

789. Intentionally left blank.

790. Intentionally left blank.

791. Intentionally left blank.

4.3.4.3.1.4 The Mapper Server Had a Vulnerability that Could Be Exploited To Steal FTP Usernames and Passwords

792. In May 2010, ProviDyn detected a Level 2 vulnerability in the FTP application on Mapper of "FTP Supports Clear Text Authentication." (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21).

Response to Finding No. 792

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

793. The FTP Supports Clear Text Authentication vulnerability means that the FTP application on Mapper was set up not to encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer or a man-in-the-middle attack. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 20; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 793

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

794. Wireshark is an example of a traffic capture or network sniffer tool. (CX0740 (Hill Report) ¶¶ 68(b), 71).

Response to Finding No. 794

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

795. ProviDyn found the FTP Supports Clear Text Authentication vulnerability was still present on Mapper during the July 2010 and September 2010 penetration tests. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 20; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 7).

Response to Finding No. 795

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

796. The CVSS severity rating included in the May, July, and September 2010 ProviDyn tests indicated that exploiting this weakness would lead to partial loss of confidentiality of information on the Mapper server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 20; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 796

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

797. ProviDyn identified a solution to the FTP Supports Clear Text Authentication vulnerability: “switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS).” (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 21; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 30; CX0061 (September 2010 ProviDyn Network Security Scan-Mapper) at 18).

Response to Finding No. 797

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was

contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

798. Intentionally left blank.

799. Intentionally left blank.

4.3.4.3.2 The Mapper Server Had Vulnerabilities In The Database Application LabMD Used To Maintain And Retrieve Sensitive Personal Information

800. MySQL is a database application LabMD used to store sensitive consumer information and to retrieve information from the database. (CX0443 (LabMD Access Letter Response by Philippa Ellis) at 6; *see also* CX0711 (Dooley, Dep. at 135-36); CX0717 (Howard, Dep. at 48); CX0735 (Kaloustian, IHT at 223-24)).

Response to Finding No. 800

Respondent has no specific response.

801. ProviDyn's May and July 2010 penetration tests of the Mapper server found that port 3306 was open and that it provided access to the Microsoft MySQL database program running on Mapper. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 5, 7; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 5, 7).

Response to Finding No. 801

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

802. The May 2010 ProviDyn penetration test found several High Risk vulnerabilities associated with the MySQL database program. These vulnerabilities are CVE 2007-5969, 5970, 6303, and 6304, all reported in the CVE in 2007 (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 20).

Response to Finding No. 802

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was

contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

803. The CVSS severity rating information included in the May 2010 ProviDyn penetration test noted that exploiting these vulnerabilities leads to partial compromise of the confidentiality, integrity, and availability of the Mapper server. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 20).

Response to Finding No. 803

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

804. Compared to the May 2010 ProviDyn penetration test, the July 2010 test identified a new, different High Risk vulnerability associated with the MySQL database program. This vulnerability is CVE 2009-0819, reported in 2009. **(**CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 804

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

805. The CVSS severity rating information included in the July 2010 ProviDyn penetration test noted that the new vulnerability is easy to exploit, leading to partial loss of the availability of the Mapper server. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 805

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy. Moreover, Respondent further objects to this proposed finding of fact because it misstates the record–the cited reference does not state that it is "easy to exploit."

806. A solution to all of these vulnerabilities in the MySQL database program has been known for years: install an updated version of the MySQL program on Mapper. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 20; CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 19).

Response to Finding No. 806

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy. Moreover, Respondent further objects to this proposed finding of fact because it misstates the record–the cited reference does not state "a solution has been known for years."

807. NVD (at CVE-2007-5969) published details about the MySQL vulnerability and how to remediate it in 2007. (CX0070 (May 2010 ProviDyn Network Security Scan – Mapper) at 20; *see also* CX0740 (Hill Report) at 63 (citing NVD CVE-2007-5969 vulnerability, http://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2007-5969)).

Response to Finding No. 807

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

808. Information about the MySQL vulnerabilities, including remediation, was available to information technology practitioners starting in 2007. (CX0740 (Hill Report) at 63 (citing NVD CVE-2007-5969 vulnerability, http://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2007-5969)).

Response to Finding No. 808

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

809. Intentionally left blank.

810. Intentionally left blank.

4.4 LabMD Did Not Use Adequate Measures to Prevent Employees From Accessing Personal Information Not Needed to Perform Their Jobs

4.4.1 LabMD Did Not Implement Access Controls

811. LabMD did not use readily available access controls to prevent employees from accessing Personal Information not needed to perform their jobs. (*Infra* §§ 5.4.1.1 (LabMD Employees Had Access to Sensitive Information that They Did Not Need to Perform Their Jobs) (¶¶ 817-821), 5.4.1.2 (LabMD Sales Representatives Had Access to Patient Medical Records) (¶¶ 824-827)).

Response to Finding No. 811

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

812. As part of a layered data security strategy, companies that maintain sensitive information should restrict access to that data by defining roles for their employees and specifying the types of data that are needed by employees in those roles. (CX0740 (Hill Report) ¶ 83).

<u>Response to Finding No. 812</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

813. A company that does not limit employees' access to sensitive information increases the likelihood that the data will be exposed outside of the organization, either by a malicious insider or in a compromise of the computer network. (CX0740 (Hill Report) ¶ 81; Hill, Tr. at 165-66).

<u>Response to Finding No. 813</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

814. Companies can use operating system functionalities and other applications to limit employees' access to information. (CX0740 (Hill Report) ¶ 85).

<u>Response to Finding No. 814</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

815. Intentionally left blank.

816. Intentionally left blank.

4.4.1.1 LabMD Employees Had Access to Sensitive Information that They Did Not Need to Perform Their Jobs.

817. LabMD did not limit its employees' access to sensitive information to that which was needed to perform their jobs. (*Infra* ¶¶ 818-821).

<u>Response to Finding No. 817</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

818. LabMD cannot specify the exact information to which its employees had access, stating only that its employees had "various levels of access" to Personal Information. (CX0763 (LabMD's Revised Response to Interrogs. 1 and 2); CX0764 (LabMD's Second Rev. Resp. to Interrogs. 1 and 2)).

<u>Response to Finding No. 818</u>

Respondent objects to this finding of fact because it is unsupported by the citations to the record. The citations to the record do not support the claim that LabMD cannot specify the exact information to which its employees had access. Rather, the sources provide that a **specific list** of employees had "various levels of access" to **specific information**.

819. Nothing prevented staff from accessing the information of patients for which they had no job-related need. (CX0706 (Brown, Dep. at 117-18)).

Response to Finding No. 819

Respondent objects to this proposed finding of fact because it is inaccurate and ignores contradictory testimony in the evidentiary record. Employees only had access to what they needed to do their jobs and could not install without administrative privileges. (CX 0707 (Bureau, Dep. at 79-80)).

According to Harris only billing personnel could access Lytec billing system. (CX0716 (Harris, Dep. at 75)). It was necessary for billing personnel to have access to LabSoft in order to do their jobs. (CX0716 (Harris, Dep. at 72-74)).

820. All billing personnel had full access to patient and lab databases, which allowed them to access all of a patient's Personal Information, including lab results. (CX0706 (Brown, Dep. at 116-18); CX0715-A (Gilbreth, Dep. at 21); CX0711 (Dooley, Dep. at 133-34)).

Response to Finding No. 820

Respondent objects to this proposed finding of fact to the extent it suggests that Billing employees did not require access to all patient information in order to do their jobs. Employees only had access to what they needed to do their jobs and could not install without administrative privileges. (CX0707 (Bureau, Dep. at 79-80)).

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. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 46-47)).

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. (CX0706 (Brown, Dep. at 117-118, 153)).

According to Harris only billing personnel could access Lytec billing system. (CX0716 (Harris, Dep. at 75)). It was necessary for billing personnel to have access to LabSoft in order to do their jobs. (CX0716 (Harris, Dep. at 72-74)).

821. LabMD turned off the feature of its laboratory information software, LabSoft, that allowed for distinct access settings for different users. (CX0717 (Howard, Dep. at 117)).

Response to Finding No. 821

Respondent has no specific response.

822. Intentionally left blank.

823. Intentionally left blank.

4.4.1.2 LabMD Sales Representatives Had Access to Patient Medical Records

824. LabMD sales representatives has access to patient medical records, including test results. (*Infra* ¶¶ 825-827).

Response to Finding No. 824

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

825. Sales representatives were able to use physician-clients' login credentials to log in to LabSoft. (CX0718 (Hudson, Dep. at 73-74, 88-89, 183)).

Response to Finding No. 825

Respondent objects to this proposed finding of fact to the extent it ignores pertinent facts explaining that sales representatives only were able to access LabSoft with physicians' office credentials and permission. (CX0718 (Hudson, Dep. at 183)).

826. Sales representatives could log in to LabMD's computer network using their own credentials to access pathology reports and the volume of specimens sent in from particular doctors. (CX0722 (Knox, Dep. at 61-62)).

Response to Finding No. 826

Respondent objects to this proposed finding of fact to the extent it ignores pertinent facts contradicting whether Knox actually had the ability to access reports using his credentials without the credentials and permission of physician clients.

"So, yes I had administrative rights to that specific laptop, but I didn't have administrative rights to get onto my laptop to log in to LabMD's servers and go in–go into their servers. I didn't have those administrative rights." (CX0722 (Knox, Dep. at 56)).

Q. And what is your understanding of what you could access with your user ID and password?

A. I don't recall everything I could look up. I know I could look up–for example, if a doctor would call me and ask me about a report, I had the capabilities of looking to see if that report was pending or completed.

(CX0722 (Knox, Dep. at 57)).

827. In more than one instance, sales representatives used a physician-client's login credentials to demonstrate the ordering process to a different prospective physician-client. (CX0718 (Hudson, Dep. at 73-75, 90-91)). Sales representatives had access to a "demo data" account for demonstration purposes, but would use another practices' account in some instances if the other physician consented. (CX0718 (Hudson, Dep. at 90-91)).

Response to Finding No. 827

Respondent has no specific response.

828. Intentionally left blank.

829. Intentionally left blank.

4.4.2 Data Minimization

830. If an organization collects more data than needed to conduct its business, it increases the scope of potential harm if the organization's network is compromised. (Hill, Tr. at 165-66; CX0740 (Hill Report) ¶ 79).

Response to Finding No. 830

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

831. IT practitioners regularly purged unneeded data throughout the Relevant Time Period. (CX0740 (Hill Report) ¶ 80(b)).

Response to Finding No. 831

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

832. LabMD collected and maintained more information on its network than was necessary for it to conduct its business. (*Infra* §§ 5.4.2.1 (LabMD Had No Policy for Deleting Personal Information and Maintained the Information Indefinitely) (¶¶ 835-841), 5.4.2.2 (LabMD Collected Personal Information for Which It Had No Business Need) (¶¶ 844-849); CX0740 (Hill Report) ¶ 80). Because employees could access the Personal Information of any consumer on LabMD's network, even those to whom LabMD provided no services, LabMD did not use adequate measures to prevent employees from having access to Personal Information that was not needed to perform their jobs and increased the likelihood that the data would be exposed. (CX0740 (Hill Report) ¶ 80).

Response to Finding No. 832

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

833. Intentionally left blank.

834. Intentionally left blank.

4.4.2.1 LabMD Had No Policy for Deleting Personal Information and Maintained the Information Indefinitely

835. LabMD had no policy for deleting patient information and maintained that information indefinitely. (*Infra* ¶¶ 836-841).

Response to Finding No. 835

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

836. LabMD does not delete or destroy Personal Information of consumers, but maintains it indefinitely. (CX0710-A (Daugherty, LabMD Designee, Dep. at 60, 215-16, 220-21)).

Response to Finding No. 836

Respondent has no specific response.

837. LabMD has not destroyed any billing information it has received from consumers since the company's inception. (CX0733 (Boyle, LabMD Designee, IHT) at 39-40);

(CX0443 (2/24/2010 Access Letter Response) at 6); (CX0717 (Howard, Dep. at 113)).

Response to Finding No. 837

Respondent has no specific response.

838. LabMD imported data from legacy systems into the systems currently in use. (CX0443 (2/24/2010 Access Letter Response) at 6).

Response to Finding No. 838

Respondent has no specific response.

839. LabMD had no deletion policy and has not destroyed any information maintained in its Laboratory Information System. (CX0717 (Howard, Dep. at 113); CX0725-A (Martin, Dep. at 68; CX0715-A (Gilbreth, Dep. at 27); CX0731 (Truett, Dep. at 60)).

Response to Finding No. 839

Respondent has no specific response.

840. LabMD had no retention policy for day sheets and retained them indefinitely. (CX0733 (Boyle, IHT at 36-37); CX0710-A (Daugherty, LabMD Designee, Dep. at 60); CX0715-A (Gilbreth, Dep. at 42-44)).

Response to Finding No. 840

Respondent objects to this proposed finding of fact to the extent it ignores the fact that LabMD’s retention policy was to maintain the documentation indefinitely.

841. LabMD retained payment information it received from consumers, including copies of personal checks and credit and debit payment card account numbers, indefinitely. (*Supra* §§ 4.6.2.6.1 (Credit Cards) (¶¶ 134-138), 4.6.2.6.2 (Personal Checks) (¶¶ 140-148)).

Response to Finding No. 841

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that “[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”); *see also* at 3 (stating

"[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

842. Intentionally left blank.

843. Intentionally left blank.

4.4.2.2 LabMD Collected Personal Information for Which It Had No Business Need

844. LabMD collected information on thousands of patients for whom it never provided testing and for which it had no business need. (*Infra* ¶¶ 845-849).

Response to Finding No. 844

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

845. LabMD imported into its network Personal Information of patients for whom it never provided testing from its physician-clients. (CX0718 (Hudson, Dep. at 24-25, 52-54, 59-62); CX0726 (Maxey, SUN Designee, Dep. at 45, 80); CX0725-A (Martin, Dep. at 58); CX0715-A (Gilbreth, Dep. at 22-23); *supra* § 4.6.2 (Collection of Consumers' Personal Information From Physician-Clients) *et seq.* (¶¶ 81-120)).

Response to Finding No. 845

Respondent has no specific response.

846. Information collected from physician-clients included full name, date of birth, address, Social Security number, and diagnosis codes used for that patient. (CX0718 (Hudson, Dep. at 59-60, 61-62); CX0725-A (Martin, Dep. at 69); (CX0706 (Brown, Dep. at 17-18); CX0715-A (Gilbreth, Dep. at 11, 37-38)).

Response to Finding No. 846

Respondent has no specific response.

847. LabMD maintained Personal Information on over 750,000 patients. (CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) at 5, Adm. 23).

Response to Finding No. 847

Respondent has no specific response.

848. Approximately 20% to 25% of the patients whose information LabMD collected or maintained never had any testing performed by LabMD. CX0710-A (Daugherty, LabMD Designee, Dep. at 198).

Response to Finding No. 848

Respondent has no specific response.

849. LabMD collected and maintained indefinitely Personal Information regarding approximately 100,000 consumers for whom it never performed testing. (JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 3 (LabMD maintained information on more than 750,000 patients); CX0710-A (Daugherty, LabMD Designee, Dep. at 198) (20 to 25% of patients in database had never had any testing performed by LabMD)).

Response to Finding No. 849

Respondent has no specific response.

850. Intentionally left blank.

851. Intentionally left blank.

4.5 LabMD Did Not Adequately Train Employees to Safeguard Personal Information

852. LabMD did not adequately train its employees to safeguard Personal Information. (Hill, Tr. 167; CX0740 (Hill Report) ¶ 91; *infra* §§ 5.5.1 (LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information) (¶¶ 857-863), 5.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information) (¶¶ 866-869), 5.5.2.1 (LabMD's Compliance Training Did Not Adequately Train Employees to Safeguard Personal Information) (¶¶ 872-876), 5.5.2.2 (LabMD Provided No Other Trainings on LabMD Policies or Procedures to Safeguard Personal Information) (¶¶ 879-884), 5.5.2.2.1 (LabMD IT Employees Did Not Provide Information Security Training to Non-IT Employees) (¶¶ 887-891)).

Response to Finding No. 852

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

853. Proper training is integral to a reasonable layered data security strategy. (Hill, Tr. 169-70).

<u>Response to Finding No. 853</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

854. Information security training is important because users are the weakest link in any information security program. (CX0740 (Hill Report) ¶ 87; Hill, Tr. 169-70).

<u>Response to Finding No. 854</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

855. Intentionally left blank.

856. Intentionally left blank.

4.5.1 LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information

857. A company should provide its IT employees with periodic training on protecting against evolving threats. (Hill, Tr. 167-68; CX0740 (Hill Report) ¶ 89).

Response to Finding No. 857

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

858. Resources for training IT employees in data security were available at low cost during the Relevant Time Period. (Hill, Tr. 173-74; CX0740 (Hill Report) ¶¶ 89 n.30, 92).

Response to Finding No. 858

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

859. A company should also provide information security training to enable its IT employees to define and implement a comprehensive information security plan. (Hill, Tr. 167-70).

Response to Finding No. 859

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

860. LabMD failed to provide adequate training to its IT employees to safeguard Personal Information. (Hill, Tr. 170; CX0740 (Hill Report) ¶ 91; *infra* ¶¶ 861-862).

Response to Finding No. 860

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

861. LabMD did not provide its IT employees with information security-related training or training regarding security threats. (CX0717 (Howard, Dep. at 23-26); CX0711 (Dooley, Dep. at 148-49); CX0724 (Maire, Dep. at 29, 31); CX0707 (Bureau, Dep. at 37-38); CX0719 (Hyer, Dep. at 160-62): CX0705-A (Bradley, Dep. at 147, 152); CX0735 (Kaloustian, IHT at 208-09); CX0734 (Simmons, IHT at 60-62)).

Response to Finding No. 861

Respondent objects to this proposed finding of fact because it ignores clear evidence in the record to the contrary. Hyer testified that he trained two main staff people to the level they needed to be to accomplish what they were doing in Bradley as a desktop person and Parr as network administrator. "Not specifically security issues as much as discipline and structure in the IT world, you know as it should be run." (CX0719 (Hyer, Dep. at 130)).

862. LabMD's IT contractor prior to March 2007, APT, did not provide security training. (CX0731 (Truett, Dep. at 125)).

Response to Finding No. 862

Respondent has no specific response.

863. As a result of a lack of training for its IT employees, LabMD's security practices were reactive, incomplete, *ad hoc*, and ineffective. (Hill, Tr. 171-72; CX0740 (Hill Report) ¶ 91).

Response to Finding No. 863

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

864. Intentionally left blank.

865. Intentionally left blank.

4.5.2 LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information

866. LabMD failed to adequately train its non-IT employees to safeguard Personal Information. (Hill, Tr. 171; CX0740 (Hill Report) ¶ 90; *infra* §§ 5.5.2.1 (LabMD's Compliance Training Did Not Adequately Train Employees to Safeguard Personal Information) (¶¶ 872-876), 5.5.2.2 (LabMD Provided No Other Trainings on LabMD Policies or Procedures to Safeguard Personal Information) (¶¶ 879-884), 5.5.2.2.1

(LabMD IT Employees Did Not Provide Information Security Training to Non-IT Employees) (¶¶ 887-891)).

Response to Finding No. 866

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

867. A company should provide its employees with training regarding any security mechanisms that require employee action—such as antivirus programs they must run themselves—or that employees are not technically prevented from reconfiguring. (Hill, Tr. 168-69; CX0740 (Hill Report) ¶¶ 87, 88).

Response to Finding No. 867

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

868. Employees should also receive periodic training on acceptable use of computer equipment, current threats, and best practices. (CX0740 (Hill Report) ¶¶ 87, 89).

Response to Finding No. 868

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

869. Information security training is especially necessary where employees are given administrative access to equipment, because they can reconfigure the equipment in ways that could result in compromises such as downloading unauthorized software. (Hill, Tr. 168-69; CX0740 (Hill Report) ¶ 87). Training is needed to inform employees of the consequences of making changes to equipment. (Hill, Tr. 168-69; CX0740 (Hill Report) ¶¶ 90, 104(a)).

Response to Finding No. 869

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

870. Intentionally left blank.

871. Intentionally left blank.

4.5.2.1 LabMD's Compliance Training Did Not Adequately Train Employees to Safeguard Personal Information

872. The compliance training LabMD provided to employees did not adequately train employees to safeguard Personal Information. (*Infra* ¶¶ 873-876).

Response to Finding No. 872

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

873. Ms. Carmichael, a consultant who put LabMD's Compliance Program in place, developed compliance training for LabMD. (CX0708 (Carmichael, Dep. at 22-23)).

Response to Finding No. 873

Respondent has no specific response.

874. Ms. Carmichael created a training PowerPoint presentation for her and others to use when providing compliance training to LabMD employees. (CX0708 (Carmichael, Dep. at 26); *see* CX0127 (Compliance Training PowerPoint Slides).

Response to Finding No. 874

Respondent has no specific response.

875. In conjunction with a few slides, the compliance training that Ms. Carmichael provided stated that LabMD had obligations with regard to Personal Information and information security. (CX0708 (Carmichael, Dep. at 28, 41-42, 45-46, 55-57, 58); CX0127 (Training PowerPoint Slides) at 9-12, 15-17, 21; CX0722 (Knox, Dep. at 47-48, 50)).

Response to Finding No. 875

Respondent has no specific response.

876. The compliance training did not train LabMD employees about LabMD's information security practices. (CX0708 (Carmichael, Dep. at 25-26, 42, 46-49, 55-61); CX0707 (Bureau, Dep. at 105)).

Response to Finding No. 876

Respondent has no specific response.

877. Intentionally left blank.

878. Intentionally left blank.

4.5.2.2 LabMD Provided No Other Trainings on LabMD Policies or Procedures to Safeguard Personal Information

879. Besides the Compliance Training, LabMD did not provide any other training to employees on how to safeguard Personal Information. (*Infra* ¶¶ 881-884).

Response to Finding No. 879

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

880. Many LabMD employees could change security settings on their computers because they were given administrative rights over their workstations or laptop computers. (CX0717 (Howard, Dep. at 19-20); CX0735 (Kaloustian, IHT at 166-70, 187-89); CX0724 (Maire, Dep. at 60-61, 80); CX0705-A (Bradley, Dep. at 147-49); CX0722 (Knox, Dep. at 54-55); CX0719 (Hyer, Dep. at 28-31)).

Response to Finding No. 880

Respondent has no specific response.

881. LabMD did not provide its non-IT employees, including sales representatives, with any training regarding security mechanisms or the consequences of reconfiguring security settings in applications. (CX0705-A (Bradley, Dep. at 145-47); CX0706 (Brown, Dep. at 90-93); CX0711 (Dooley, Dep. at 148); CX0714-A ([Fmr. LabMD Empl.], Dep. at 85-87; 96-97); CX0718 (Hudson, Dep. at 52-54, 73); CX0719 (Hyer, Dep. at 160-62); CX0716 (Harris, Dep. at 45); CX0724 (Maire, Dep. at 32); CX0734 (Simmons, IHT at 61-62); CX0735 (Kaloustian, IHT at 128-30, 214-15)).

Response to Finding No. 881

Respondent has no specific response.

882. Billing employees were able to access sensitive patient information, but were given no instructions about keeping that information private or on limiting their access to that needed for the performance of their job. (CX0706 (Brown, Dep. at 96-99)).

Response to Finding No. 882

Respondent objects to this proposed finding of fact because it is inaccurate due to contradictory testimony in the evidentiary record.

On a yearly basis LabMD employees received training on LabMD compliance standards, HIPAA compliance, limited use of computer systems restricting use of internet and prohibition against playing CDs or downloading of information from the internet. (CX0716 (Harris, Dep. at 62)).

Fmr. LabMD Empl signed the LabMD, Inc. Employee Handbook Receipt Acknowledgement in 2007 when she started her employment. (CX0130 (LabMD Handbook, at 003839)). At that time she also received HIPAA training by watching a video on privacy concerns and HIPAA violations. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 86)).

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

883. Ms. Brown, billing manager from 2005 through 2006, relied on the training that her employees received in their previous employment rather than providing training at LabMD. (CX0706 (Brown, Dep. at 98)).

Response to Finding No. 883

Respondent objects to this proposed finding of fact because it mischaracterizes testimony in the evidentiary record.

> Q. And when you were the manager training other employees, you didn't train them on information security?
>
> A. No, because the employees that I hired had worked at other medical offices, so as far as HIPAA guidelines and things of that nature, they had to have had that background before they started working for me.

(CX0706 (Brown, Dep. at 91)).

884. Ms. Brown supervised several college students with no previous experience and she provided them with no formal training. (CX0706 (Brown, Dep. at 99-100)). Although the college students were not permitted to deal with patients directly, they were given full access to the patient database. (CX0706 (Brown, Dep. at 99-100)).

Response to Finding No. 884

Respondent objects to this proposed finding of fact because it ignores testimony in the evidentiary record regarding training of college students and attempts to mislead the Court by stating that college students had full access to the patient database when the evidence in the record is that college students only had access to Lytec. (CX0706 (Brown, Dep. at 101)).

> Q. How did the college students learn about what they were to do with respect to patient privacy?
>
> A. They were trained.
>
> Q. By who?
>
> A. By myself.

(CX0706 (Brown, Dep. at 99)).

885. Intentionally left blank.

886. Intentionally left blank.

4.5.2.2.1 LabMD IT Employees Did Not Provide Information Security Training to Non-IT Employees

887. LabMD's IT employees did not train LabMD's non-IT employees on information security. (CX0724 (Maire, Dep. at 31, 34); CX0717 (Howard, Dep. at 24-26); CX0707 (Bureau, Dep. at 41); CX0711 (Dooley, Dep. at 148); CX0719 (Hyer, Dep. at 160-61); *infra* ¶¶ 888-891).

<u>Response to Finding No. 887</u>

Respondent has no specific response.

888. Mr. Howard only trained other LabMD employees on LabSoft software and how to refill printers. (CX0717 (Howard, Dep. at 24)). He trained one pathologist who occasionally had a software virus on his workstation on how to remove it. (CX0717 (Howard, Dep. at 24-25)).

<u>Response to Finding No. 888</u>

Respondent has no specific response.

889. Mr. Hyer only provided training to IT employees Mr. Bradley and Ms. Parr, and the accounting manager. (CX0719 (Hyer, Dep. at 159-60)).

<u>Response to Finding No. 889</u>

Respondent has no specific response.

890. Mr. Hyer provided training to the LabMD accounting manager to help use IT to reduce her workload. (CX0719 (Hyer, Dep. at 160)).

<u>Response to Finding No. 890</u>

Respondent has no specific response.

891. None of training that Mr. Hyer provided to the accounting manager involved security issues. (CX0719 (Hyer, Dep. at 160-61)).

<u>Response to Finding No. 891</u>

Respondent has no specific response.

892. Intentionally left blank.

893. Intentionally left blank.

4.5.2.3 LabMD's Written Policies and Documentation Did Not Provide Instruction to Employees on How to Safeguard Personal Information

894. LabMD's written documentation did not adequately instruct employees on how to safeguard Personal Information. (*Infra* ¶¶ 895-900).

Response to Finding No. 894

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

895. LabMD's Employee Handbook and Compliance Program do not provide instruction on how to safeguard Personal Information. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6; CX0005 (LabMD Compliance Program effective Jan. 2003) at 4).

Response to Finding No. 895

Respondent objects to this finding of fact because it is unsupported by the citation to the record. LabMD's Employee Handbook expressly states that employees "are required to share information only with authorized individuals and only for specific, authorized reasons."

896. LabMD's Employee Handbook does not contain specific policies about protecting data resources and infrastructure, or explain what, if any, mechanisms LabMD implemented to achieve the goal. (CX0740 (Hill Report) ¶ 61(a); Hill, Tr. 129; CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6).

Response to Finding No. 896

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

897. Although the Employee Handbook states that LabMD "has taken specific measures to ensure [its] compliance" with HIPAA, employees were not informed what these measures were and were given no specific instructions for complying with the law. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6; CX0706 (Brown, Dep. at 94-96, 105); CX0715-A (Gilbreth, Dep. at 83-84); CX0714-A ([Fmr. LabMD Empl.], Dep. at 88); CX0716 (Harris, Dep. at 51); CX0707 (Bureau, Dep. at 26); CX0719 (Hyer, Dep. at 163)).

Response to Finding No. 897

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "To be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014)*)*.

898. When LabMD provided its Employee Handbook to employees, no one went through it to explain any policies within it or any HIPAA guidelines. (CX0707 (Bureau, Dep. at 24-25); CX0706 (Brown, Dep. at 102-05); CX0714-A ([Fmr. LabMD Empl.], Dep. at 88); CX0716 (Harris, Dep. at 48)).

Response to Finding No. 898

Respondent objects to this proposed finding of fact because it is an attempt to mislead the Court by suggesting that no explanation of LabMD's policies were available if necessary. Gilbreth testifies that she would train new employees using the Employee Handbook. This training could last anywhere from an half hour to an hour and a half. Those employees would be provided the Handbook , and asked to read it. Particular areas were highlighted, "using personal email was unacceptable…" "And they would be asked if they had any questions." (CX 0715(Gilbreth, Dep. at 82-83)).

Respondent objects to this proposed finding of fact because it is wholly irrelevant to these proceedings. "To be sure, the Commission cannot enforce HIPAA and does not seek to do so." Commission Order Denying LabMD's Motion to Dismiss, *In the Matter of LabMD, Inc.,* FTC Dkt. No. 9357, at 12 (Jan. 16, 2014).

899. In July 2010, LabMD contends that it completed the education and training of LabMD managers and employees regarding CX0007, LabMD's Computer Hardware, Software and Data Usage and Security Policy Manual. (CX0445 (LabMD Access Letter Response by Philippa Ellis) at 6).

Response to Finding No. 899

Respondent has no specific response.

900. However, when LabMD provided its policy manuals created in 2010, CX0006 and CX0007, to Ms. Brown, as of January 2014 she was only given copies of the manuals and told to sign them; nothing was done to ensure that the employee actually read and understood the manuals. (CX0706 (Brown, Dep. at 86-91)).

Response to Finding No. 900

Respondent objects to this proposed finding of fact because it ignores testimony in the evidentiary record where Brown testifies that she was given the manuals to read and given an opportunity to ask questions before signing and giving it back to John Boyle. (CX0706 (Brown, Dep. at 85-89)).

901. Intentionally left blank.

902. Intentionally left blank.

4.6 LabMD Did Not Require Common Authentication-Related Security Measures

903. As part of a layered data security strategy, companies should use strong authentication mechanisms to control access to computers, services, applications, and data. (CX0740 (Hill Report) ¶¶ 25-26, 94).

Response to Finding No. 903

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited paragraphs contemplate "authentication mechanisms to control access to workstations," but not access to computers, services, applications, and data. (CX0740 (Hill Report) ¶¶ 25-26, 94)).

904. To authenticate themselves, users provide information to a system that tells the system who they are and then proves that identity. (CX0740 (Hill Report) ¶ 25).

Response to Finding No. 904

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

905. Usernames and passwords are a common authentication mechanism. (Hill, Tr. 176; CX0740 (Hill Report) ¶ 94).

Response to Finding No. 905

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's expert report actually states at ¶ 94 that "usernames/passwords are **one such** [authentication] mechanism…" (emphasis added).

906. The effectiveness of usernames and passwords depends on: (1) the strength of the passwords; and (2) how the passwords are stored and managed. (CX0740 (Hill Report) ¶ 94; Hill, Tr. 177-79).

<u>Response to Finding No. 906</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

907. Intentionally left blank.

908. Intentionally left blank.

4.6.1 LabMD Did Not Adopt and Implement Policies Prohibiting Employees From Using Weak Passwords

909. Without strong password policies, an intruder may guess a weak password and use it to impersonate an employee and obtain unauthorized access to computers and information. (Hill, Tr. 177-78, 180-82; *see also* CX0740 (Hill Report) ¶¶ 55, 94).

<u>Response to Finding No. 909</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

910. LabMD did not require employees to use common, effective authentication-related security measures, and its authentication mechanisms were not reasonable for securing its network. (CX0740 (Hill Report) ¶¶ 95, 95(a); Hill, Tr. 176; *infra* §§ 5.6.1.1 (LabMD Did Not Have Written Policies For Strong Passwords) (¶¶ 919-923), 5.6.1.2 (LabMD Did Not Implement and Follow Practices Requiring Employees

> to Use Strong Passwords)(¶¶ 926-931), 5.6.2 (LabMD Did Not Have Enforcement Mechanisms to Ensure Its Employees Used Reasonable Password Practices) *et seq.* (¶¶ 934-966), 5.6.3 (LabMD Did Not Implement Strong Password Policies for its Servers) (¶¶ 968-971), 5.6.4 (LabMD Allowed Weak Passwords to Be Used on Computers Placed in Physician-Clients' Offices) (¶¶ 974-983), 5.6.6 (LabMD Did Not Implement Alternatives to Requiring Strong Passwords) (¶¶ 990-993).

Response to Finding No. 910

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.) Moreover, Respondent objects to this proposed finding of fact because it improperly cites to expert testimony to support factual propositions that should be established by fact witnesses or documents. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015); *see also In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Lastly, Respondent objects to this proposed finding of fact to the extent Complaint

Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

911. Mr. Hyer, who joined LabMD in 2009 to provide IT services, stated that prior to his arrival, LabMD's password practices were "less than adequate" and that existing controls "were not being enforced." (CX0719 (Hyer, Dep. at 25)).

Response to Finding No. 911

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Mr. Hyer actually stated on page 25 of his deposition that " . . there were **some** less than adequate controls enforced by the IT manager." (emphasis added). Mr. Hyer said nothing about the adequacy of password practices. (CX0719 (Hyer, Dep. at 25)).

912. To promote the effectiveness of usernames/passwords, a company should have policies on how to create strong passwords. (CX0740 (Hill Report) ¶¶ 31(d), 94; Hill, Tr. 131-32). Without strong password policies, it is likely that an attacker will be able to guess a password and gain access to the system. (Hill, Tr. 176-77).

Response to Finding No. 912

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

913. Mr. Hyer stated that LabMD's passwords were "not as complex as they should have been." (CX0719 (Hyer, Dep. at 26-27)).

Response to Finding No. 913

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Mr. Hyer actually stated, "[a]lso, the passwords were **probably** not as complex as they should have been **and that's because people can't remember complex passwords**." (emphasis added). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the dates of Mr. Hyer's employment with LabMD. Hyer worked for LabMD from June 2009 to March 2012. (CX0719 (Hyer, Dep. at 143).

914. A company should impose minimum requirements for password length, required characters (including numbers, case, and symbols), how long passwords can be used before the user is required to change, password history, and passwords to avoid. (CX0740 (Hill Report) ¶ 94; *see* Hill, Tr. 177-78).

<u>Response to Finding No. 914</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

915. Dictionary words are inherently weak passwords. (CX0740 (Hill Report) ¶ 87).

<u>Response to Finding No. 915</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Dr. Hill's expert report actually states at ¶ 87 that "[w]eak passwords… that contain dictionary words… are more easily guessed than others." Paragraph 87 does not state that dictionary words are inherently weak passwords.

916. LabMD did not establish password policies to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network. (Hill, Tr. 176, 179-80; CX0740 (Hill Report) ¶ 95; *infra* §§ 5.6.1.1 (LabMD Did Not Have Written Policies for Strong Passwords) (¶¶ 919-924), 5.6.1.2 (LabMD Did Not Implement and Follow Practices Requiring Employees to Use Strong Passwords) (¶¶ 926-931), 5.6.2 (LabMD Did Not Have Enforcement Mechanisms to Ensure Its Employees Used Reasonable Password Practices) *et seq.* (¶¶ 934-966).

Response to Finding No. 916

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

917. Intentionally left blank.

918. Intentionally left blank.

4.6.1.1 LabMD Did Not Have Written Policies For Strong Passwords

919. LabMD did not establish password policies or implement enforcement mechanisms to ensure that strong passwords were being used to authenticate users

and authorize them to access LabMD's network. (Hill, Tr. 176, 179-80; CX0740 (Hill Report) ¶ 95; *infra* ¶¶ 920-923; §§ 5.6.1.2 (LabMD Did Not Implement and Follow Practices Requiring Employees to Use Strong Passwords) (¶¶ 926-931), 5.6.2 (LabMD Did Not Have Enforcement Mechanisms to Ensure Its Employees Used Reasonable Password Practices) *et seq.* (934-966), 5.6.3 (LabMD Did Not Implement Strong Password Policies for Its Servers) (¶¶ 968-971), 5.6.4 (LabMD Allowed Weak Passwords to Be Used on Computers Placed in Physician-Clients' Offices) (¶¶ 974-983)).

Response to Finding No. 919

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.) Moreover, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

920. LabMD did not have a written policy prohibiting use of the same characters for the username and password. (CX0711 (Dooley, Dep. at 58); CX0733 (Boyle, LabMD Designee, IHT at 184); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual)

at 24; *see also supra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) (¶¶ 415-417), 5.2.2.1.1 (LabMD's Employee Handbook Was Not a Comprehensive Written Information Security Program) (¶ 426), 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program (¶¶ 436-437); CX0710-A (Daugherty, LabMD Designee, Dep. at 119)).

Response to Finding No. 920

Respondent has no specific response.

921. LabMD did not have a written policy regarding password complexity. (CX0733 (Boyle, LabMD Designee, IHT at 183); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1); CX0707 (Bureau, Dep. at 82-83); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24; CX0710-A (Daugherty, LabMD Designee, Dep. at 119); *see also supra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) (¶¶ 415-417), 5.2.2.1.1 (LabMD's Employee Handbook Was Not a Comprehensive Written Information Security Program) (¶ 426), 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program (¶¶ 436-437)).

Response to Finding No. 921

Respondent has no specific response.

922. LabMD did not have a written policy prohibiting the use of dictionary words as passwords. (CX0733 (Boyle, LabMD Designee, IHT at 185-86); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24) ; CX0710-A (Daugherty, LabMD Designee, Dep. at 119); *see also supra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) (¶¶ 415-417), 5.2.2.1.1 (LabMD's Employee Handbook Was Not a Comprehensive Written Information Security Program) (¶ 426), 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program (¶¶ 436-437)).

Response to Finding No. 922

Respondent has no specific response.

923. LabMD did not have a written policy prohibiting users from using the same username and password across applications. (CX0707 (Bureau, Dep. at 82-83); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24) ; CX0710-A (Daugherty, LabMD Designee, Dep. at 119); *see also supra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) (¶¶ 415-417), 5.2.2.1.1 (LabMD's Employee Handbook Was Not a Comprehensive Written Information

Security Program) (¶ 426), 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program (¶¶ 436-437)).

Response to Finding No. 923

Respondent has no specific response.

924. Intentionally left blank.

925. Intentionally left blank.

4.6.1.2 LabMD Did Not Implement and Follow Practices Requiring Employees to Use Strong Passwords

926. LabMD did not have a password policy – written or unwritten – in place before November 2010, when it centralized its password management. (CX0707 (Bureau, Dep. at 82); CX0715-A (Gilbreth, Dep. at 67); CX0705-A (Bradley, Dep. at 128-29)).

Response to Finding No. 926

Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable prior to 2007. Brandon Bradley worked for LabMD from May 2010 until February 7, 2014. (CX0705-A (Bradley, Dep. at 7-8)). Matt Bureau worked for LabMD from December 2008 through April 2010. (CX0707 (Bureau, Dep. at 7)). Billing employee Patricia Gilbreth, who later became a billing manager, was employed from 2007 to 2013 at LabMD. (CX0715-A (Gilbreth, Dep. at 6)). Thus, given that none of these employees were employed by LabMD prior to 2007, it cannot be verified that LabMD did not have a password policy in place prior to 2007. Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel ignores the fact that LabMD's User Account Policy contained password policies requiring employees to change their password from the default password. (CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 21).

927. From at least October 2006 through August 2009, LabMD did not require complex passwords for the applications its employees used. (CX0735 (Kaloustian, IHT at 255-56); CX0734 (Simmons, IHT at 151-54, 156-57)).

Response to Finding No. 927

Respondent has no specific response.

928. LabMD did not have a policy requiring a minimum password length for desktop credentials prior to centralizing password management in November 2010. (CX0733 (Boyle, LabMD Designee, IHT at 181); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1); CX0707 (Bureau, Dep. at 82); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24); *see also* CX0710-A (Daugherty, LabMD Designee, Dep. at 119)).

Response to Finding No. 928

Respondent has no specific response.

929. LabMD did not have a policy requiring users to include numbers or special characters in their passwords prior to centralizing password management in November 2010. (CX0727-A (Parr, Dep. at 110-12); CX0715-A (Gilbreth, Dep. at 67); CX0711 (Dooley, Dep. at 56-57, 59-60); CX0707 (Bureau, Dep. at 82-83); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1); *see also* CX0710-A (Daugherty, LabMD Designee, Dep. at 119) (Employee Handbook does not include password policies)).

Response to Finding No. 929

Respondent has no specific response.

930. When Mr. Hyer began working at LabMD full time as Director of IT in approximately August 2009, LabMD's Employee User Account Policy, which required employees to change their password from the default password they were initially given, was not enforced. (CX0719 (Hyer, Dep. at 74-75); *see* CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 21).

Response to Finding No. 930

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Mr. Hyer did not state that policies which required employees to change their password from the default password were not enforced; rather, he stated that there was "multiple use of the same log-in and password by employees in the laboratory." (CX0719 (Hyer, Dep. at 75).

931. In November 2010, LabMD centralized its management of passwords. (CX0313 (LabMD IT Project Outline - Network, Hardware, Software changes) at 1; CX0727-A (Parr, Dep. at 110-12); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1); CX0705-A (Bradley, Dep. at 69-70)).

Response to Finding No. 931

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The record does not state that LabMD centralized management of passwords of in November 2010, rather Jennifer Parr stated that the new password requirements went into place "[p]rior to November 2nd, 2010…" (CX0727-A (Parr, Dep. at 112)). Moreover, regarding timing of the implementation of centralized passwords, Brandon Bradley stated, "your guess is as good as mine. I don't know." (CX0705-A (Bradley, Dep. at 69-70).

932. Intentionally left blank.

933. Intentionally left blank.

4.6.2 LabMD Did Not Have Enforcement Mechanisms to Ensure Its Employees Used Reasonable Password Practices

934. LabMD did not implement enforcement mechanisms to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network. (Hill, Tr. 176, 179-80; CX0740 (Hill Report) ¶ 95; *infra* §§ 5.6.2.1 (LabMD Employees Used Weak Passwords) (¶¶ 945-951); 5.6.2.2 (LabMD Did Not Prevent Employees From Using the Same Password for Years) (¶¶ 954-957); 5.6.2.3 (LabMD Employees Were Not Prevented from Sharing Authentication Credentials) (¶¶ 960-963), 5.6.2.4 (LabMD Did Not Require Passwords in All Instances) (¶ 966)).

Response to Finding No. 934

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.). Moreover, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

935. To ensure reasonable password policies are enforced, a company's password management should be centralized. (CX0740 (Hill Report) ¶ 94).

<u>Response to Finding No. 935</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

936. Passwords should not be stored in clear text, rather a cryptographic hash should be applied to the password before it is stored. (CX0740 (Hill Report) ¶ 94; Hill, Tr. 178-79).

Response to Finding No. 936

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

937. The Windows operating system includes a centralized scheme to manage passwords. (CX0740 (Hill Report) ¶ 95(a)).

Response to Finding No. 937

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

938. LabMD did not use that centralized scheme, Active Directory, included in its Windows XP Operating Systems to manage passwords. (CX0719 (Hyer, Dep. at 84-88); CX0735 (Kaloustian, IHT at 166-67, 171-72)).

Response to Finding No. 938

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. At pages 84-88 of his deposition, Hyer discusses the fact that he used Active Directory to automate the expiration of passwords. Kaloustian states at page 166 of his deposition "…later on in the process, ….we finally kind of formalized our active directory rights." Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the dates of Mr. Hyer and Mr. Kaloustian's employment with LabMD. Hyer worked for LabMD from June 2009 to March 2012. (CX0719 (Hyer, Dep. at 143). Curt Kaloustian worked for LabMD from October 2006 through April or May 2009. (CX0735 (Kaloustian, IHT at 7, 17)).

939. Active Directory can be used to automatically expire passwords and force them to be changed and to limit a user's access to programs or resources. (CX0719 (Hyer, Dep. at 84-87); CX0735 (Kaloustian, IHT at 166-67, 171-72)).

Response to Finding No. 939

Respondent has no specific response.

940. LabMD did not switch to using central management for password and user management until November 2010. (CX0313 (LabMD IT Project Outline - Network, Hardware, Software changes) at 1; CX0727-A (Parr, Dep. at 110-12); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1); CX0705-A (Bradley, Dep. at 69-70)).

Response to Finding No. 940

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The record does not state that LabMD centralized management of passwords in November 2010, rather Jennifer Parr stated that the new password requirements went into place "[p]rior to November 2nd, 2010…" (CX0727-A (Parr, Dep. at 112). And regarding timing of the implementation of centralized passwords, Brandon Bradley stated, "your guess is as good as mine. I don't know." (CX0705-A (Bradley, Dep. at 69-70). Moreover, Hyer states that LabMD centralized management of passwords in Summer 2009. (CX0719 (Hyer, Dep. at 84)).

941. Prior to implementing centralized password management in November 2010, LabMD did not have a process to assess the strength of employee passwords. (CX0735 (Kaloustian, IHT at 257); CX0734 (Simmons, IHT at 153); CX0727-A (Parr, Dep. at 111-12); CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login.msg) at 1).

<u>Response to Finding No. 941</u>

Respondent objects to this proposed finding because it inaccurately states that LabMD began implementing centralized password management in November 2010. Actually, the record reflects that LabMD implemented centralized password management "[p]rior to November 2nd, 2010…" (CX0727-A (Parr, Dep. at 112)).

942. Prior to implementing central password management, LabMD IT employees verified that users were implementing new password requirements adopted in 2010 or 2011 by asking users to tell the IT person their password. (CX0705-A (Bradley, Dep. at 69-72)).

<u>Response to Finding No. 942</u>

Respondent has no specific response.

943. Intentionally left blank.

944. Intentionally left blank.

4.6.2.1 LabMD Employees Used Weak Passwords

945. LabMD employees used weak passwords to access LabMD's network, on site and remotely. (*Infra* ¶¶ 946-951).

<u>Response to Finding No. 945</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

946. LabMD employees used passwords that were not sufficiently complex, used only letters, were too short, and were easily guessed. (CX0705-A (Bradley, Dep. at 125-26); CX0719 (Hyer, Dep. at 26-27)).

Response to Finding No. 946

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Neither Mr. Bradley nor Mr. Hyer stated that LabMD passwords were not sufficiently complex. When asked whether "LabMD" is a secure password, Mr. Bradley stated "possibly not." (CX0705-A (Bradley, Dep. at 125-26). Furthermore, Mr. Hyer actually stated, "[a]lso, the passwords were **probably** not as complex as they should have been **and that's because people can't remember complex passwords**." (CX0719 (Hyer, Dep. at 26-27)) (emphasis added). Moreover, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the dates of Mr. Bradley and Mr. Hyer's employment with LabMD. Brandon Bradley worked for LabMD from May 2010 until February 7, 2014. (CX0705-A (Bradley, Dep. at 7-8)). Hyer worked for LabMD from June 2009 to March 2012. (CX0719 (Hyer, Dep. at 143).

947. LabMD Employee Sandra Brown used the username, sbrown, and password, labmd, to access her LabMD computer on site. (CX0706 (Brown, Dep. at 13); CX0167 (PC Tracking (John) Spreadsheet)).

Response to Finding No. 947

Respondent has no specific response.

948. Ms. Brown's credentials were assigned to her by LabMD. (CX0706 (Brown, Dep. at 15)).

Response to Finding No. 948

Respondent has no specific response.

949. Ms. Brown worked from home using her own computer and a service, Logmein.com, that allowed her to access LabMD's system remotely. (CX0706 (Brown, Dep. at 10-11)).

Response to Finding No. 949

Respondent has no specific response.

950. Ms. Brown's user name and password for logmein.com were also "sbrown" and "labmd," respectively. (CX0706 (Brown, Dep. at 10-11); CX0167 (PC Tracking (John) Spreadsheet)).

Response to Finding No. 950

Respondent has no specific response.

951. Logmein.com allows users to access LabMD's system, including patient databases. (CX0706 (Brown, Dep. at 11-12)). At least six employees used "labmd" as a password. (CX0167 (PC Tracking (John) Spreadsheet); CX0705-A (Bradley, Dep. at 125-26)).

Response to Finding No. 951

Respondent objects to Complaint Counsel's statement that "Logmein.com allows users to access LabMD's system, including patient databases" as it is overly broad, fails to define "users", and misstates the record. Brown did not state that any logmein user could access LabMD's system; rather, she stated that she utilized logmein.com to "pull up the screen that shows the desktop at work," which then enabled her to gain access to "the Lytec system." (CX0706 (Brown, Dep. at 11)).

Respondent has no specific response to Complaint Counsel's statement that "[a]t least six employees used 'labmd' as a password."

952. Intentionally left blank.

953. Intentionally left blank.

4.6.2.2 LabMD Did Not Prevent Employees From Using the Same Passwords for Years

954. Users who have access to highly sensitive information should change their passwords frequently. (Hill, Tr. 178; CX0740 (Hill Report) ¶ 94).

Response to Finding No. 954

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

955. Prior to 2010, LabMD had no policy that passwords needed to be changed periodically. (CX0705-A (Bradley, Dep. at 69-70, 128); CX0006 (LabMD Policy Manual) at 14 (no requirement for expiration of passwords); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24 (policy put in practice in 2010); CX0734 (Simmons, IHT at 152)).

<u>Response to Finding No. 955</u>

Respondent has no specific response.

956. LabMD did not have a written policy prohibiting password reuse. (CX0733 (Boyle, LabMD Designee, IHT at 183); CX0006 (LabMD Policy Manual) at 14; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 24); *see also supra* §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) (¶¶ 415-417), 5.2.2.1.1 (LabMD's Employee Handbook Was Not a Comprehensive Written Information Security Program) (¶ 426), 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program (¶¶ 436-437)).

<u>Response to Finding No. 956</u>

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Mr. Boyle did not state that LabMD did not have a written policy prohibiting password use. Rather, when asked about a specific policy, Mr. Boyle stated "[t]his policy does not [prohibit from reusing passwords]." (CX0733(Boyle (LabMD Designee) IHT, at 183)).

957. Ms. Brown used her credentials "sbrown" and "labmd," respectively, to access her LabMD computer on site and remotely, unchanged, from 2006 to 2013. (CX0706 (Brown, Dep. at 13)).

Response to Finding No. 957

Respondent has no specific response.

958. Intentionally left blank.

959. Intentionally left blank.

4.6.2.3 LabMD Employees Were Not Prevented from Sharing Authentication Credentials

960. LabMD employees were not prevented from sharing authentication credentials. (*Infra* ¶ 962).

Response to Finding No. 960

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

961. Mr. Hyer stated that LabMD's practice of allowing users to share log-ons was "an absolute no no in an IT environment." (CX0719 (Hyer, Dep. at 26)).

Response to Finding No. 961

Respondent has no specific response.

962. Between at least October 2006 and August 2009, some LabMD employees shared passwords that were used to access Personal Information, including logins used to access desktop computers on the LabMD network. (CX0719 (Hyer, Dep. at 26-27, 45, 74-75); CX0735 (Kaloustian, IHT at 79, 295)).

Response to Finding No. 962

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record that give a timeframe for when "some LabMD employees shared passwords."

963. At least six employees used "LabMD" as a password. (CX0167 (PC Tracking (John) Spreadsheet); CX0705-A (Bradley, Dep. at 125-26)).

Response to Finding No. 963

Respondent has no specific response.

964. Intentionally left blank.

965. Intentionally left blank.

4.6.2.4 LabMD Did Not Require Passwords in All Instances

966. From October 2006 through August 2009, LabMD employee workstations could be accessed as "guest" with some program functionality available. (CX0730 (Simmons, Dep. at 113-14)).

Response to Finding No. 966

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Simmons' testimony is limited to a discussion regarding access to Rosalind Woodson's computer in which she states that with "Widows XP you could log in as a guest and you still would have been able to use [Limewire] from [Ros's] computer," but that she was "not positive" that there was guest functionality on Ros's computer. (CX0730 (Simmons, Dep. at 113-14)).

967. Intentionally left blank.

4.6.3 LabMD Did Not Implement Strong Password Policies for Its Servers

968. LabMD also did not implement strong password policies for its network infrastructure, including servers. (*Infra* ¶¶ 969-971).

Response to Finding No. 968

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

969. As of August 2009, LabMD's LabNet server used a login username of "admin" and password "bulldog." (CX0248 (Email M. Bureau to J. Boyle Subject: Walk Arounds 8/14/09, with Attachments) at 5).

Response to Finding No. 969

Respondent has no specific response.

970. From October 2006 through April 2009, every server login username was "admin," and every password was "LABMD." (CX0735 (Kaloustian, IHT at 294-96)).

Response to Finding No. 970

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross-examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD,* FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.")

971. The servers were all linked to the same default administrator user profile, preventing IT staff from setting up user accounts for each IT employee. (CX0735 (Kaloustian, IHT at 295-96)).

Response to Finding No. 971

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.")

972. Intentionally left blank.

973. Intentionally left blank.

4.6.4 LabMD Allowed Weak Passwords to Be Used on Computers Placed in Physician-Clients' Offices

974. LabMD created or allowed weak passwords for the user accounts and logins of its physician-clients to LabMD's software for ordering tests and retrieving results. (Hill, Tr. 185-87; CX0740 (Hill Report) ¶ 95(a); *infra* ¶¶ 975-983).

Response to Finding No. 974

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.). Moreover, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

975. When computers were set up in physician-clients' offices, the clients would submit the employees that needed access to the computer, so that LabMD could set up accounts for those individuals. (CX0718 (Hudson, Dep. at 85-86)).

Response to Finding No. 975

Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the dates of Ms. Hudson's employment with LabMD. Lawrence Hudson worked for LabMD from approximately January or February 2004 through June or July 2007 as a territory manager. (CX0718 (Hudson, Dep. at 14-15)).

976. The credentials to log on to the computers supplied to LabMD's physician-clients were selected by the clients, and LabMD did not have a process to evaluate the complexity of the credentials. (CX0730 (Simmons, Dep. at 75-76); CX0734 (Simmons, IHT at 47-48); CX0718 (Hudson, Dep. at 86-88)).

Response to Finding No. 976

Respondent has no specific response.

977. LabMD would not reject any requested user credentials. (CX0728 (Randolph (Midtown Urology Designee), Dep. at 39-41)).

Response to Finding No. 977

Respondent objects to this proposed finding of fact because it is overly broad and misstates the record. Randolph was the Midtown Urology Designee, and thus can only make statements that bind Midtown Urology–not other LabMD clients. While Randolph did state that LabMD did not reject Midtown Urology's requested username and password, this statement is only biding on Midtown Urology.

978. From October 2006 through August 2009, LabMD typically made nurses' passwords their initials at its physician-clients' offices. (CX0734 (Simmons, IHT at 151-52, 154-55)).

Response to Finding No. 978

Respondent has no specific response.

979. The passwords typically created for users in the physician-clients' offices included the user's initials. (CX0734 (Simmons, IHT at 151-55); CX0718 (Hudson, Dep. at 85-88)).

Response to Finding No. 979

Respondent has no specific response.

980. There was no policy prohibiting users from using their user name as their password for the doctors' offices. (CX0711 (Dooley, Dep. at 58); CX0718 (Hudson, Dep. at 85-88); CX0728 (Randolph, Midtown Urology Designee, Dep. at 40-41).

Response to Finding No. 980

Respondent has no specific response.

981. In some cases, the login credentials requested by LabMD's physician-clients used the username as a password. (CX0718 (Hudson, Dep. at 87-88)). In other cases, the username might be a nurse's initials, and the password the initials repeated twice. CX0734 (Simmons, IHT at 154-55)).

Response to Finding No. 981

Respondent has no specific response.

982. From October 2006 to April 2009, LabMD's physician-clients would generally have a username and password shared among many users. (CX0735 (Kaloustian, IHT at 302-03)).

<u>Response to Finding No. 982</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.")

983. In some instances, all of the employees at a physician-clients' practice would share one set of login credentials to access the operating system of a LabMD-provided computer. (CX0728 (Randolph, Midtown Urology Designee, Dep. at 38-41)).

<u>Response to Finding No. 983</u>

Respondent objects to this proposed finding of fact because it is overly broad and misstates the record. Randolph was the Midtown Urology Designee, and thus can only make statements that bind Midtown Urology–not other LabMD clients. While Randolph did state that Midtown Urology employees shared one set of login credentials, this statement is only biding on Midtown Urology.

984. Intentionally left blank.

985. Intentionally left blank.

4.6.5 LabMD Did Not Disable the Accounts of Former Users

986. Prior to August 2009, LabMD failed to deactivate the login access of past clients that no longer needed access, and former clients could still access the LabMD network. (CX0719 (Hyer, Dep. at 35-37, 40-41)).

<u>Response to Finding No. 986</u>

Respondent has no specific response.

987. In July 2010, Managed Data Solutions assisted LabMD with a network assessment of some of its servers. (CX0479 (MDS Server Assessment) at 1). The assessment found several users whose passwords do not expire, including Administrator, Guest, TsInternetUser, IUSR-LABMD-23, IWAM_LABMD-23, ASPNET, and asimmons. (CX0479 (MDS Server Assessment) at 58). Ms. Simmons had left LabMD almost a year prior to the scan, in August 2009. (*Supra* § 4.8.20 (Alison Simmons) (¶ 371)).

Response to Finding No. 987

Respondent objects Complaint Counsel's statement that "Ms. Simmons had left LabMD almost a year prior to the scan, in August 2009" because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

988. Intentionally left blank.

989. Intentionally left blank.

4.6.6 LabMD Did Not Implement Alternatives to Requiring Strong Passwords

990. Two-factor authentication is an authentication mechanism requiring two forms of proof, such as a password (something the user knows) and a biometric, such as a fingerprint or iris scan, or a token (something the user possesses). (CX0740 (Hill Report) ¶ 25).

Response to Finding No. 990

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

991. Two-factor authentication is used as part of a layered data security strategy to reduce the risk of compromise. It is often used in connection with remote login or access to highly sensitive data. (CX0740 (Hill Report) ¶ 25).

Response to Finding No. 991

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

992. LabMD did not use two-factor authentication for remote users. (CX0707 (Bureau, Dep. at 83-84); CX0722 (Knox, Dep. at 62-63); CX0718 (Hudson, Dep. at 73-74, 89, 183); CX0734 (Simmons, IHT at 47-48, 144, 156); CX0735 (Kaloustian, IHT at 257-58).

Response to Finding No. 992

Respondent has no specific response.

993. Two-factor authentication could have compensated for LabMD's failure to require the use of strong passwords for remote login. (Hill, Tr. at 184-85; CX0740 (Hill Report) ¶ 95(a)).

Response to Finding No. 993

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

994. Intentionally left blank.

995. Intentionally left blank.

4.7 LabMD Did Not Maintain and Update Operating Systems and Other Devices

996. LabMD did not maintain and update operating systems of computers and other devices on its network. (CX0740 (Hill Report) ¶ 99; Hill, Tr. 189). Through at least 2010, LabMD did not update its operating systems and other applications in a timely manner to address risks and vulnerabilities. (CX0740 (Hill Report) ¶ 99; Hill, Tr. 189; *infra* §§ 5.7.1 (Some LabMD Servers Used a Windows Operating System Years After Microsoft Had Stopped Updating and Supporting It) *et seq.* (¶¶ 1003-1028), 5.7.2 (LabMD Used Insecure SSL 2.0 for Three Years After Updates Were Recommended) (¶¶ 1031-1040), 5.7.3 (LabMD Had No Policy to Update Network Hardware Devices) (¶ 1043)).

Response to Finding No. 996

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Paragraph 99 of Dr. Hill's report discusses hackers exploitations of software bugs generally, with no specific application to LabMD. At Tr. 189, Dr. Hill discusses mitigating risks created by software applications. T hus, Complaint Counsel's citation to the record does not support its statement that "LabMD did not maintain and update operating systems of computers and other devices on its network." Furthermore, Dr. Hill stated that "… LabMD did not update its operating systems and other applications in a timely manner to address risk **and vulnerabilities in those software applications."** (emphasis added, explaining the narrow context of Complaint's Counsel's statement in its proposed findings of fact).

997. Maintaining and updating operating systems of computers and other devices to protect against known vulnerabilities is integral to a company's layered data security strategy. (CX0740 (Hill Report) ¶ 99; Hill, Tr. 189-90).

Response to Finding No. 997

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. In ¶ 99 of her report and on pages 189-90 of her transcript, Dr. Hill does not mention whether maintaining and updating operating systems is **integral to a company's**

layered data security strategy; rather she states "[t]o limit [a hacker's] exploits, IT practitioners should connect to product notification systems and immediately apply remediation processes and updates for vulnerabilities that have been identified." (CX0740 (Hill Report) ¶ 99).

998. Bugs are endemic to complex software, and attackers exploit software bugs to gain unauthorized access to consumers' Personal Information. (CX0740 (Hill Report) ¶¶ 98-99; Hill, Tr. 189-90).

Response to Finding No. 998

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

999. Hackers exploit software bugs to gain unauthorized access to computer resources and data. (CX0740 (Hill Report) ¶ 99).

Response to Finding No. 999

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1000. Upon starting at LabMD, [Former LabMD Employee] was issued a desktop computer. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 27)). The operating system on the computer was never updated during the time [Former LabMD Employee] worked at LabMD. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 34)).

Response to Finding No. 1000

Respondent has no specific response.

1001. Intentionally left blank.

1002. Intentionally left blank.

4.7.1 Some LabMD Servers Used a Windows Operating System Years After Microsoft Had Stopped Updating and Supporting It

1003. LabMD servers were running software with vulnerabilities that had been identified and reported by the security and IT community several years prior to being detected on LabMD computers. (CX0740 (Hill Report) ¶ 100(a); Hill, Tr. 190-94); *infra* ¶¶ 1004-1008; §§ 5.7.1.1 (Unpatched Vulnerabilities in the Veritas Backup Application on the LabNet Server) *et seq.* (¶¶ 1011-1028).

Response to Finding No. 1003

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010"). Moreover, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

1004. Windows vulnerabilities were the single largest threat identified in ProviDyn's May 21, 2010 scan of LabMD's Mapper server. (CX0070 (May 2010 ProviDyn Network Security Scan – Mapper) at 2).

Response to Finding No. 1004

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. The chart of page 2 of CX0070 references shows "how the **potential security threats** are spread across different families of threat classifications." (emphasis added). This graph does not assess the significance or magnitude of threats, and thus does not conclude, as Complaint Counsel suggests, that "Windows vulnerabilities were the single largest threat identified in ProviDyn's May 21, 2010 scan …" Moreover, Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1005. LabMD failed to update servers running Windows NT 4.0 for two years after Windows ceased to support the operating system. (Hill, Tr. 190; CX0740 (Hill Report) ¶ 100(c); *infra* ¶¶ 1006-1008).

Response to Finding No. 1005

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to this proposed finding of fact because it improperly cites to expert testimony to support factual propositions that should be established by fact witnesses or documents. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015).

Respondent further objects to this proposed finding of fact because Dr. Hill's statement at ¶ 100 of her report (*i.e.* "Record evidence shows that LabMD's servers were running the Windows NT 4.0 server in 2006, two years after the product had been retired by Microsoft.") is solely predicated on Curt Kaloustian's testimony. Curt Kaloustian's testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

1006. In December 2004, Microsoft recommended that customers migrate their servers to "'more secure Microsoft Operating system products as soon as possible"' because Microsoft retired its support for Windows NT 4.0. (CX0740 (Hill Report) ¶ 100(c)).

Response to Finding No. 1006

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1007. The support life-cycle for Windows NT 4.0 ended on June 30, 2004. (CX0740 (Hill Report) ¶ 100(c), 100(c) n.50).

Response to Finding No. 1007

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1008. Some LabMD servers, such as the LabNet server, were running the Windows NT 4.0 operating system in 2006. (CX0735 (Kaloustian, IHT at 271-74)).

Response to Finding No. 1008

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Complaint Counsel's citation does not state when Windows NT 4.0 operating system was running.

1009. Intentionally left blank.

1010. Intentionally left blank.

4.7.1.1 Unpatched Vulnerabilities in the Veritas Backup Application on the LabNet Server

1011. LabMD's LabNet server had multiple vulnerabilities that could have been corrected by free updates from software vendors made available years before ProviDyn discovered them for LabMD. (*Infra* §§ 5.7.1.1.1 (The Veritas Backup Application Was Configured With the Default Administrative Password) (¶¶ 1017-1021), 5.7.1.1.2 (The Veritas Backup Application Had a Buffer Overflow Vulnerability) (¶¶ 1021-1028)).

<u>Response to Finding No. 1011</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1012. LabMD's LabNet server stores and handles large amounts of consumers' sensitive Personal Information, including specific diagnoses and laboratory results. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 8-9, Resp. to Interrog. 14; CX0710-A (Daugherty, LabMD Designee, Dep. at 193)).

<u>Response to Finding No. 1012</u>

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Neither Response to Interrog. 14 of LabMD's Second Set of Discovery Responses, nor page 193 of Mr. Daugherty's LabMD Designee deposition discuss the amount of information stored on the LabNet server.

1013. The LabNet server used Veritas backup software. (CX0724 (Maire Dep. Tr.) at 22-23; CX0735 (Kaloustian, IHT at 285-87)).

<u>Response to Finding No. 1013</u>

Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Neither Mr. Maire's deposition transcript at pages 22-23, nor Mr.

Kaloustian's investigational hearing transcript at pages 285-287 state that the LabNet server used Veritas backup software.

1014. ProviDyn concluded that the "Overall Security Posture" of the LabNet server was "Poor" in May 2010. (CX0067 (ProviDyn Network Security Scan - LabNet) at 1).

Response to Finding No. 1014

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1015. Intentionally left blank.

1016. Intentionally left blank.

4.7.1.1.1 The Veritas Backup Application Was Configured With the Default Administrative Password

1017. In May 2010 the Veritas backup software on the LabNet server was configured with the default administrative password. (CX0067 (ProviDyn Network Security Scan - LabNet) at 22).

Response to Finding No. 1017

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1018. ProviDyn identified the default administrative password vulnerability as a Level 5, or "Urgent Risk," which means that an attacker can compromise the entire host. (CX0067 (ProviDyn Network Security Scan - LabNet) at 22, 65; CX0740 (Hill Report) ¶ 100(d)).

Response to Finding No. 1018

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp* II, Ltd., 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1019. A solution to this vulnerability had been identified as early as August 15, 2005. (CX0740 (Hill Report) ¶ 100(d); CX0067 (ProviDyn Network Security Scan - LabNet) at 22 (referencing CVE-2005-2611)).

Response to Finding No. 1019

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1020. The solution to the vulnerability was to update the product in accordance with the vendor advisory on the issue. (CX0067 (ProviDyn Network Security Scan - LabNet) at 22).

Response to Finding No. 1020

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1021. The updates that would have corrected this vulnerability would be available to LabMD at no cost. (Hill, Tr. 194).

Response to Finding No. 1021

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1022. Intentionally left blank.

1023. Intentionally left blank.

4.7.1.1.2 The Veritas Backup Application Had a Buffer Overflow Vulnerability

1024. The LabNet server's Veritas backup software also had a "buffer overflow" vulnerability, which an attacker could have exploited along with the default administrative password vulnerability. (CX0067 (ProviDyn Network Security Scan - LabNet) at 22-23).

Response to Finding No. 1024

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1025. The buffer overflow vulnerability gave an attacker the ability to execute code remotely in order to take over partial control of that server. (CX0067 (ProviDyn Network Security Scan - LabNet) at 22; CX0740 (Hill Report) ¶ 100(d); Hill, Tr. 193).

Response to Finding No. 1025

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp* II, Ltd.,2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1026. ProviDyn identified the "buffer overflow" vulnerability as a level 4, or "Critical Risk." (CX0067 (ProviDyn Network Security Scan – LabNet) at 22, 65).

Response to Finding No. 1026

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1027. Warnings about the "buffer overflow" vulnerability had been published in 2007. (Hill, Tr. 193-94; CX0740 (Hill Report) ¶ 100(d); CX0067 (ProviDyn Network Security Scan – LabNet) at 22-23 (referencing CVE-2007-3509)).

Response to Finding No. 1027

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1028. LabMD could have corrected this vulnerability by downloading a free update from the vendor when the solution was made available in 2007. (Hill, Tr. 193-94).

Response to Finding No. 1028

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1029. Intentionally left blank.

1030. Intentionally left blank.

4.7.2 LabMD Used Insecure SSL 2.0 for Three Years After Updates Were Recommended

1031. LabMD ran servers with an insecure version of SSL for three years after Microsoft instructed users to remedy this vulnerability. (*Infra* ¶¶ 1032-1039).

Response to Finding No. 1031

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1032. Secure Socket Layer Protocol (SSL) is the means by which data is encrypted during transmission over the Internet using HTTPS. (CX0740 (Hill Report) ¶ 61(c) n.14).

Response to Finding No. 1032

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1033. Two of LabMD's servers— the LabNet and Mail servers—ran software that used an insecure version of the Secure Socket Layer Protocol, SSL 2.0. (CX0067 (ProviDyn Network Security Scan – LabNet) at 23-24; CX0068 (ProviDyn Network Security Scan – Mail) at 31).

Response to Finding No. 1033

Respondent objects to this proposed finding of fact because it is merely a statement Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1034. ProviDyn rated this SSL vulnerability as a level 3, "High Risk." (CX0067 (ProviDyn Network Security Scan – LabNet) at 23, 65; CX0068 (ProviDyn Network Security Scan – Mail) at 31, 73).

Response to Finding No. 1034

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1035. This vulnerability provided hackers with access to specific information on the host, including security settings. (CX0740 (Hill Report) ¶ 100(e)).

Response to Finding No. 1035

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1036. SSL 2.0 had been deprecated for several years. (CX0067 (ProviDyn Network Security Scan-LabNet) at 23-24; CX0068 (ProviDyn Network Security Scan – Mail) at 31).

Response to Finding No. 1036

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1037. An attacker may be able to exploit this vulnerability to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients. (CX0067 (ProviDyn Network Security Scan-LabNet) at 23-24; CX0068 (ProviDyn Network Security Scan – Mail) at 31).

Response to Finding No. 1037

Respondent objects to this proposed finding of fact to the extent that it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1038. Microsoft provided instructions on how to disable SSL 2.0 as early as April 23, 2007. (CX0740 (Hill Report) ¶ 100(e); CX0737 (Hill Rebuttal Report) ¶ 29 n.45).

Response to Finding No. 1038

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1039. Microsoft also released Windows Server 2008 on February 27, 2008, and recommended that users upgrade to this operating system to address the SSL 2.0 flaw. (CX0740 (Hill Report) ¶ 100(e); CX0737 (Hill Rebuttal Report) ¶ 29 n.45).

Response to Finding No. 1039

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1040. LabMD could have easily addressed this vulnerability by following instructions provided by Microsoft. (CX0737 (Hill Rebuttal Report) ¶ 29 n.45).

Response to Finding No. 1040

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1041. Intentionally left blank.

1042. Intentionally left blank.

4.7.3 LabMD Had No Policy to Update Network Hardware Devices

1043. LabMD had no written policy in place to update the software of hardware devices such as firewalls and routers. (CX0006 (LabMD Policy Manual) at 13, 18 (no hardware updating policy); CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 22-23, 31-32 (no hardware updating policy)).

Response to Finding No. 1043

Respondent has no specific response.

1044. Intentionally left blank.

4.8 LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information

1045. A layered data security strategy must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker and detect unauthorized access when an attack is successful. (CX0740 (Hill Report) ¶ 103; Hill, Tr. 195).

Response to Finding No. 1045

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. Dr. Hill actually states that "**a defense in depth strategy** must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker and detect unauthorized access when an attack is successful." (emphasis added) (distinction made because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report). Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1046. The process of detection enables the organization to identify and patch holes in its security system. (CX0740 (Hill Report) ¶ 103; Hill, Tr. 195).

Response to Finding No. 1046

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1047. LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. (Hill, Tr. 194-95; CX0740 (Hill Report) ¶ 105; *infra* §§ 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1050-1063), 5.8.2 (LabMD Stored Backups of Personal Information on an Employee Workstation) (¶¶ 1066-1072); 5.8.3 (LabMD Did Not Reasonably Deploy Firewalls) *et seq.* (¶¶ 1075-1105), 5.8.4 (LabMD Did Not Deploy Automated Scanning Mechanisms, Such as a File Integrity Monitor) (¶¶ 1108-1110)).

Response to Finding No. 1047

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

Respondent further objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter* *of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see* also at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that infra or supra should also not be used).

1048. Intentionally left blank.

1049. Intentionally left blank.

4.8.1 LabMD Employees Were Given Administrative Access to Workstation Computers

1050. Employees should be given non-administrative accounts on workstations. (CX0740 (Hill Report) ¶ 104(a); Hill, Tr. 195-96).

Response to Finding No. 1050

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1051. Administrative access gives a user full control over a computer, including the ability to download software onto that computer. (Hill, Tr. 101-02; CX0740 (Hill Report) ¶ 104(a)). Non-administrative accounts give users limited control over their computers, which prevents the inadvertent downloading of software that could compromise not only their system but compromise the entire network. (Hill, Tr. 196).

Response to Finding No. 1051

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1052. Downloading an unauthorized application for which there is no business need is a risk because it introduces a vulnerability in the network. The application could have malicious software embedded within it and the individual downloading it may not understand the consequences of the download. (Hill, Tr. 97-98).

Response to Finding No. 1052

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1053. When employees are given non-administrative accounts on their workstation computers, they are prevented from installing software on the workstation. (Hill, Tr. 195-96; CX0740 (Hill Report) ¶ 104(a); *see also* Hill, Tr. 199 (noting that billing manager's administrative access allowed her to download LimeWire to her workstation).

Response to Finding No. 1053

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1054. The Windows operating system used on LabMD computers included functionality for assigning non-administrative accounts to users. (CX0740 (Hill Report) ¶ 104(a); Hill, Tr. 202).

Response to Finding No. 1054

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp* II, Ltd.,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses.

1055. LabMD's Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual included policies requiring that most employees receive non-administrative rights (employee user profiles) over their computers. (CX0006 (LabMD Policy Manual) at 20; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 21).

Response to Finding No. 1055

Respondent has no specific response.

1056. However, at least until November 2010, many LabMD employees could change security settings on their computers because they were given administrative rights over their workstations or laptop computers. (CX0717 (Howard, Dep. at 19-20); CX0735 (Kaloustian, IHT at 166-70, 187-89); CX0724 (Maire, Dep. at 60-61, 80); CX0705-A (Bradley, Dep. at 147-49); CX0722 (Knox, Dep. at 54-56); CX0719 (Hyer, Dep. at 28-31)).

Response to Finding No. 1056

Respondent objects to this proposed finding of fact as it misstates the record, and further states that none of the citations to the record state that LabMD employees could change security settings on their passwords until **November 2010**. Moreover, Mr. Howard states that "**sometime in 2005**" he made sure that every user had their own login credentials, as opposed to everyone using the same administrative password and having administrative rights. (CX0717 (Howard, Dep. at 19-20)).

1057. Sales representatives had administrative rights to their laptops, and were able to download software. (CX0722 (Knox, Dep. at 54-56)).

Response to Finding No. 1057

Respondent objects to this proposed finding of fact because it is misstates the record and is overly broad. Mr. Knox, who was a sales representative for LabMD from 2005-2007 (CX0722 (Knox, Dep. at 15-16)), stated that he had administrative rights to his laptop, and was able to download software, (CX0722 (Knox, Dep. at 54-56)); however, this narrow statement cannot be construed as an admission that all sales representatives had administrative rights to their laptops.

1058. Employees were able to download software applications and music files from the Internet, as well as from a USB memory stick or a disk without going online. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 38-40); CX0717 (Howard, Dep. at 77); CX0735 (Kaloustian, IHT at 167); CX0724 (Maire, Dep. at 126); CX0719 (Hyer, Dep. at 28-31); CX0705-A (Bradley, Dep. at 148-49)).

Response to Finding No. 1058

Respondent objects to this proposed finding of fact because it is overbroad to the extent it suggests that all employees had access to the internet. Internet access was limited to the insurance company web sites and only managers had access to MicroSoft Outlook emails. (CX0706 (Brown, Dep. at 115; (CX0706 (Brown, Dep. at 121)). Ms. Harris describes her access to the internet as limited to insurance companies or otherwise being blocked. (CX0716 (Harris, Dep. at 82-83)). Simmons states that billing could not download anything from the internet and their internet access was blocked. (CX0730 (Simmons, Dep. at 22-26, 38-43)).

1059. LabMD allowed managers, IT department employees, secretaries, and sales representatives with administrative access accounts to use their computers to go online and did not place restrictions on the sites they could visit online. (CX0735 (Kaloustian, IHT at 136-37).

Response to Finding No. 1059

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent’s counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel’s use of Kaloustian testimony, this Court stated

"… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."). Moreover, Respondent objects to this proposed finding of fact because it ignores evidence in the record to the contrary. Internet access was limited to the insurance company web sites and only managers had access to MicroSoft Outlook emails. (CX0706 (Brown, Dep. at 115; (CX0706 (Brown, Dep. at 121)). Billing Employee Gilbreth was employed as finance manager by LabMD and later became billing manager from August 2007 to December 2013. (CX0715-A (Gilbreth, Dep. at 6, 72). There were restrictions on access to the internet and there was a prohibition in the employee handbook against downloading from the internet. (CX0715-A (Gilbreth, Dep. at 63-65)). Ms. Harris describes her access to the internet as limited to insurance companies or otherwise being blocked. (CX 716 (Harris Dep. at 82-83)). Billing Employee Harris was employed by LabMD from October 2006 through January 2013. (CX0716 (Harris, Dep. at 11)).

1060. Between 2006 and August 2009, there were no firewall restrictions limiting the web sites employees in some departments could visit online. 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. (CX0730 (Simmons, Dep. at 53-54); CX0734 (Simmons, IHT at 101-02)).

Response to Finding No. 1060

Respondent objects to this proposed finding of fact because it is inaccurate due to contradictory testimony in the evidentiary record. 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). (CX0731 (Truett, Dep. at 31, 33, 41); (CX0704 (Boyle, Dep. at 49-55); (CX0685 (Boyle, CID Dep. at 112-16, 121-25, 136-38, 139-43, 152-56,199-200)). John Boyle was employed as LabMD's Vice President of Operations and General Manager form November 2006 to August 2013. (CX0704 (Boyle, Dep. at 7-8)). APT began providing services to LabMD around 2001 or 2002 and ceased providing services to LabMD in 2008 or 2009. (CX0731, (Truett, Dep. at 25, 72-73)).

Billing had a firewall and billing employees were prevented from going to nonspecified web sites, except for those needed to perform their jobs. (CX0730 (Simmons, Dep. at 16)). LabMD IT employee Simmons started with LabMD in October 2006 and left in August 2009. (RX 508 (Simmons, Dep. at 10)). Billing Employee Harris was employed by LabMD from October 2006 through January 2013. (CX0716 (Harris, Dep. at 11)). Ms. Harris describes her access to the internet as limited to insurance companies or otherwise being blocked. (CX0716 (Harris, Dep. at 82-83)).

1061. As a result of LabMD's failure to restrict employees' administrative access to workstations, LimeWire had been downloaded and installed on a computer used by LabMD's billing department manager (the "Billing Computer") in or about 2005. (Ans. ¶ 18(a); CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) at 4, Resp. to Interrog. 3; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8-9, Adms. 40-41; CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6-7; CX0150 (Screenshot: C:\) at 1; CX0730 (Simmons, Dep. at 10); CX0709 (Daugherty, Dep. at 144)).

Response to Finding No. 1061

Respondent objects to this proposed finding of fact because there is no evidence in the record that demonstrates conclusively that LimeWire was actually installed by LabMD's billing manager in 2005. Furthermore, LabMD objects this proposed finding of fact because it is an inference and not a statement of fact.

1062. This LabMD workstation had the file-sharing application LimeWire installed for years before it was discovered. (CX0730 (Simmons, Dep. at 24-25, 54-56); CX0735 (Kaloustian, IHT at 269-70); CX0711 (Dooley, Dep. at 117-19); CX0443 (LabMD Access Letter Response by Philippa Ellis) at 13).

Response to Finding No. 1062

Respondent has no specific response.

1063. There were not any defined security measures that would have prevented sharing files from the billing computer using LimeWire. (CX0730 (Simmons, Dep. at 13); CX0735 (Kaloustian, IHT at 269-70); CX0711 (Dooley, Dep. at 117-19)).

Response to Finding No. 1063

Respondent has no specific response.

1064. Intentionally left blank.

1065. Intentionally left blank.

4.8.2 LabMD Stored Backups of Personal Information on an Employee Workstation

1066. Backups containing Personal Information should be stored on devices that are isolated from other employee activities. (Hill, Tr. 196-97; CX0740 (Hill Report) ¶ 104(b)).

Response to Finding No. 1066

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1067. Backups should not be stored on employee workstations. (CX0740 (Hill Report) ¶ 104(b)).

Response to Finding No. 1067

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1068. 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)).

Response to Finding No. 1068

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1069. LabMD actively stored files containing Personal Information on employee workstations, exposing that Personal Information to unauthorized disclosure. (Hill, Tr. 196-97; CX0740 (Hill Report) ¶ 105(a); *infra* ¶¶ 1070-1072).

Response to Finding No. 1069

Respondent objects to this proposed finding of fact because it improperly cites to expert conclusion or opinion to support factual propositions that should be established by fact witnesses or documents. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015); *see also In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses.

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id*.' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used. Furthermore, Respondent objects to this proposed finding of fact because it misstates the record. Dr. Hill's report at ¶ 105(a) states only that "LabMD actively stored backups of highly sensitive Personal Information on the **Billing Manager's workstation**" and not that such information was stored generally on **employee workstations**. (emphasis added).

1070. LabMD's Policy Manuals both dictate that a copy of the backup file from LabMD's Lytec billing software should be daily saved to the Finance Manager desktop PC. (CX0006 (LabMD Policy Manual) at 10; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 14-15).

Response to Finding No. 1070

Respondent has no specific response.

1071. The daily backup of Lytec to the Finance Manager desktop PC contained all of the patient, client, and billing information related to work performed through LabMD. (CX0006 (LabMD Policy Manual) at 10; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 15).

Response to Finding No. 1071

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The manuals cited do not state that the daily backup contained "patient, client, and billing information…"

1072. LabMD also stored copies of other files with highly sensitive Personal Information, including insurance aging files, on an employee's workstation. (Daugherty, Tr. 982; CX0710-A (Daugherty, LabMD Designee, Dep. at 200); CX0730 (Simmons, Dep. at 22-26, 38-43)).

Response to Finding No. 1072

Respondent objects to this proposed finding of fact because it mischaracterizes the record. The testimony cited does not state that LabMD stored "copies of other file**s** [plural] with highly sensitive personal information …..on an employee's work station"; rather, the citations offered specifically address the 1718 file and state that it was saved on the billing manager's workstation. (Daugherty, Tr. 982).

1073. Intentionally left blank.

1074. Intentionally left blank.

4.8.3 LabMD Did Not Reasonably Deploy Firewalls

1075. A firewall is a proactive barrier protection mechanism that allows the network administrator to limit and restrict access to data in the network or on a computer. It is used to block traffic from entering the network, which can be done based on the Internet protocol address and port number (Hill, Tr. 95, 98; CX0740 (Hill Report) ¶¶ 21-22, 31(c), 104(e),(f)).

Response to Finding No. 1075

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1076. Properly configured firewalls at the network gateway and on employee workstations are part of a layered data security strategy. (CX0740 (Hill Report) ¶¶ 31(c), 104(g); *see* Hill, Tr. 199).

Response to Finding No. 1076

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd*., 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it mischaracterizes the record. Dr. Hill states that "[p]roperly configuring firewalls at the network gateway and on employee workstations implements a **defense in depth strategy** for network protection," not a layered data security strategy as Complaint Counsel suggests. This distinction is important because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

1077. A firewall should be employed at the network gateway to block all unwanted traffic from entering the network. (Hill, Tr. 197-98; CX0740 (Hill Report) ¶ 104(e)).

<u>Response to Finding No. 1077</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1078. A network gateway firewall could be configured to block traffic to all unauthorized applications, which would prevent traffic for those applications from entering the network. (CX0740 (Hill Report) ¶ 104(e); Hill, Tr. 197-98).

<u>Response to Finding No. 1078</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1079. IT practitioners during the Relevant Time Period of January 2005 through July 2010 routinely configured gateway firewalls to create a list of acceptable applications. (CX0740 (Hill Report) ¶ 104(e)).

Response to Finding No. 1079

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1080. In addition to a firewall at the network gateway, employee workstation computers should be configured to use a software firewall. (CX0740 (Hill Report) ¶ 104(f)).

Response to Finding No. 1080

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1081. Because a gateway firewall policy to block all unauthorized traffic may be difficult to implement and manage, software firewalls provide additional protection. They do so by catching errors in gateway firewall configurations and additionally filtering traffic that has passed through the gateway firewall. (CX0740 (Hill Report) ¶ 29(b)).

Response to Finding No. 1081

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1082. LabMD failed to properly deploy and configure its firewalls to block known and reasonably foreseeable threats to LabMD's network. (CX0737 (Hill Rebuttal Report) ¶ 19; CX0740 (Hill Report) ¶ 105(c); Hill, Tr. 197-98; *supra* § 5.3.2.2 (LabMD's Firewall Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 631-657); *infra* §§ 5.8.3.1 (LabMD Did Not Fully Deploy Network and Employee Workstation Firewalls) (¶¶ 1085-1091), 5.8.3.2 (LabMD Did Not Properly Configure Its Firewalls to Block IP Addresses and Unnecessary Ports) (¶¶ 1094-1105)).

Response to Finding No. 1082

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,*2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent further objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); see also at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that infra or supra should also not be used."

Respondent further objects to this proposed finding of fact because Dr. Hill's statement at ¶ 105(c) of her report (*i.e.* "Record evidence shows 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.") is solely predicated on Curt Kaloustian's testimony. Curt Kaloustian's testimony was not subjected to cross examination as Respondent’s counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel’s use of Kaloustian testimony, this Court stated “… [investigational hearing depositions are] taken without counsel, without respondent present, don’t expect them to be given a lot of weight in this proceeding.”).

1083. Intentionally left blank.

1084. Intentionally left blank.

4.8.3.1 LabMD Did Not Fully Deploy Network and Employee Workstation Firewalls

1085. LabMD failed to fully deploy firewalls, including at the network gateway and on employee workstations. (*infra* ¶¶ 1086-1087, 1089-1091).

Response to Finding No. 1085

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that “[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record”); *see also* at 3 (stating “[d]o not use ‘*Id.*’ as a cite for proposed findings of fact . . .,” implying that *infra* or *supra* should also not be used.)

1086. At LabMD’s Powers Ferry Road location, the Cypress-provided router was not configured to provide firewall protection. (CX0735 (Kaloustian, IHT at 55-56)).

Response to Finding No. 1086

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent’s counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

1087. As of October 2006, the software firewalls on LabMD's servers were disabled. (CX0735 (Kaloustian, IHT at 293-94)).

<u>Response to Finding No. 1087</u>

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding."). Moreover, Respondent objects to this proposed finding of fact because it mischaracterizes the testimony–nowhere does Mr. Kaloustian mention a date when software firewalls were disabled. Simmons testified that there were firewalls limiting internet access and blocking employees' ability to download from the internet. (CX0734 (Simmons, Dep. at 6, 125)).

1088. Employee workstations should be configured to use a software firewall. (CX0740 (Hill Report) ¶ 104(f)).

Response to Finding No. 1088

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1089. From before 2005 until at least the beginning of 2010, LabMD used Windows XP as the operating system on the computers used by its employees. (CX0707 (Bureau, Dep. at 43); CX0717 (Howard, Dep. at 97); CX0724 (Maire, Dep. at 98-99)).

Response to Finding No. 1089

Respondent has no specific response.

1090. On August 25, 2004, Microsoft released Windows XP Service Pack 2, which included Windows Firewall. (CX0740 (Hill Report) ¶ 104(f)).

Response to Finding No. 1090

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Moreover, Respondent objects to this proposed finding of fact because it is hearsay.

1091. From 2004 through March 2007, LabMD did not deploy software firewalls on LabMD employee computers and Microsoft XP's included software firewall was not configured. (CX0717 (Howard, Dep. at 101-02)).

Response to Finding No. 1091

Respondent has no specific response.

1092. Intentionally left blank.

1093. Intentionally left blank.

4.8.3.2 LabMD Did Not Properly Configure Its Firewall to Block IP Addresses and Unnecessary Ports

1094. LabMD's Network Firewalls were not configured to block unwanted traffic from entering the network. (Hill, Tr. 197-98; CX0740 (Hill Report) ¶ 105(c); *infra* ¶¶ 1095-1096, 1101-1105).

Response to Finding No. 1094

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

1095. From October 2006 through April 2009, LabMD's firewall had the capability to control network traffic by controlling or limiting the IP addresses that could communicate with LabMD's network or blocking ports network traffic can use. (CX0735 (Kaloustian, IHT at 101-03)).

Response to Finding No. 1095

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "…

[investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

1096. LabMD did not implement IP address filtering, which would prevent communication with the network by an untrusted source, until late 2008 or 2009. (CX0735 (Kaloustian, IHT at 101-03)).

Response to Finding No. 1096

Respondent objects to this proposed finding of fact as it relies exclusively upon the investigational hearing testimony of Curt Kaloustian, whose testimony was not subjected to cross examination as Respondent's counsel was not present. Therefore, the Court has stated that it will not accord this testimony much weight. *See* Final Prehearing Conference, *In the Matter of LabMD*, FTC Dkt. 9357, 9-10 (May 15, 2014) (in addressing Complaint Counsel's use of Kaloustian testimony, this Court stated "… [investigational hearing depositions are] taken without counsel, without respondent present, don't expect them to be given a lot of weight in this proceeding.").

1097. When data arrives at the destination computer, it extracts the port number from the data and sends the data to the application that corresponds to that port number. (CX0740 (Hill Report) ¶ 19).

Response to Finding No. 1097

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1098. When a port is blocked or closed, any data that arrives at the network or computer for that port will be discarded. (CX0740 (Hill Report) ¶ 22).

Response to Finding No. 1098

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1099. Firewall ports can be set up to block unwanted traffic. (Hill, Tr. 197-98).

Response to Finding No. 1099

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1100. It is important to close all ports that do not need to be open in order to prevent unauthorized access to the computer. (CX0740 (Hill Report) ¶¶ 29, 31(c); *see* Hill, Tr. 197-98).

Response to Finding No. 1100

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1101. LabMD did not configure its firewalls to block ports for which there was no business need to be open. (Hill, Tr. 197-98; CX0737 (Hill Rebuttal Report) ¶ 19; *infra* ¶¶ 1102-1105).

Response to Finding No. 1101

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests it is applicable outside of the relevant timeframe of Dr. Hill's expert opinion–January 2005 through July 2010. *See* (CX0740 (Hill Report) ¶ 4) ("This conclusion covers the time period from January 2005 through July 2010").

1102. LabMD's Veritas backup software on the LabNet server had a Level 5 vulnerability that gave an attacker administrative access to the software and the machine that was running the software, allowing the attacker to control the server and its software, and to retrieve files on the server. (CX0067 (ProviDyn Network Security Scan – LabNet) at 22; Hill, Tr. 198).

Response to Finding No. 1102

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1103. Symantec issued a warning in 2005 recommending that port 10,000 be closed until the Veritas backup application was updated to correct this vulnerability. (CX0737 (Hill Rebuttal Report) ¶ 19).

Response to Finding No. 1103

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1104. In May 2010, LabMD's LabNet server, which used Veritas backup software, had port 10,000 open. (CX0067 (ProviDyn Network Security Scan – LabNet) at 22).

Response to Finding No. 1104

Respondent objects to this proposed finding of fact because it is merely a statement contained in the ProviDyn report and is only probative of the fact that this statement was contained in the ProviDyn report and therefore should be accorded little weight as to its truth or accuracy.

1105. Veritas backup software did not need the port to be open, because backups were performed within the local area network and not across the Internet. (Hill, Tr. 198; CX0737 (Hill Rebuttal Report) ¶ 19).

Response to Finding No. 1105

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1106. Intentionally left blank.

1107. Intentionally left blank.

4.8.4 LabMD Did Not Deploy Automated Scanning Mechanisms, Such as a File Integrity Monitor

1108. File Integrity Monitoring would have contributed to a layered data security strategy. (CX0740 (Hill Report) ¶ 105(b)).

Response to Finding No. 1108

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel mischaracterizes the testimony. Dr. Hill states that "FIM therefore would have strengthened a **defense in depth approach**," as opposed to a layered data security strategy. (emphasis added). This distinction is important because Dr. Hill only became aware of the defense in depth strategy circa-mid 2009 (Hill, Tr. 306), towards the end of the Relevant Time Period for her report.

1109. File Integrity Monitoring might have detected the LimeWire file-sharing application. (Hill, Tr. 199-201; CX0740 (Hill Report) ¶ 105(b)).

Response to Finding No. 1109

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1110. LabMD did not use an automated scanning mechanism such as File Integrity Monitoring. (*Supra* § 5.3.3.2 (LabMD Did Not Implement File Integrity Monitoring) (¶¶ 705-710))

<u>Response to Finding No. 1110</u>.

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1111. Intentionally left blank.

1112. Intentionally left blank.

5. LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures

1113. LabMD could have corrected its security failures at relatively low cost using readily available security measures. (Hill, Tr. 124; CX0740 (Hill Report) ¶ 4).

<u>Response to Finding No. 1113</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1114. Intentionally left blank.

5.1 LabMD Did Not Budget for Information Technology and Data Protection Measures

1115. LabMD had no established IT budget. (CX0709 (Daugherty, Dep. at 88); CX0734 (Simmons, IHT at 51-52); CX0735 (Kaloustian, IHT at 18-19); CX0707 (Bureau, Dep. at 74).

Response to Finding No. 1115

Respondent has no specific response.

1116. LabMD IT employees had no discretion to purchase IT equipment or applications or training. (CX0734 (Simmons, IHT at 52-54); CX0707 (Bureau, Dep. at 73-74)).

Response to Finding No. 1116

Respondent has no specific response.

1117. Before purchasing IT equipment or applications or software, LabMD IT employees had to receive permission from Mr. Daugherty or Mr. Boyle to make such purchases. (CX0734 (Simmons, IHT at 52-53); CX0735 (Kaloustian, IHT at 19-23); CX0724 (Maire, Dep. at 131-33); CX0707 (Bureau, Dep. at 72-74)).

Response to Finding No. 1117

Respondent has no specific response.

1118. LabMD IT employees used low-quality products without full functionality. (CX0734 (Simmons, IHT at 113-14, 99-100 (describing limitations of free antivirus and anti-spyware products), 159-60 (same)); CX0735 (Kaloustian, IHT at 88-90, 126-28 (describing limitations of free antivirus program), 278 (explaining that inexpensive email system did not offer encryption capability)); CX0707 (Bureau, Dep. at 74-75 (describing low-quality computer parts used by LabMD))).

Response to Finding No. 1118

Respondent objects to this proposed finding of fact because it is overbroad and a conclusion, not a statement of fact.

1119. Intentionally left blank.

1120. Intentionally left blank.

5.2 Comprehensive Information Security Program

1121. LabMD could have developed, implemented, or maintained a comprehensive information security program to protect consumers' Personal Information at relatively low cost. (Hill, Tr. 132-36; CX0740 (Hill Report) ¶¶ 60 & n.8, 62).

Response to Finding No. 1121

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1122. National experts have developed best practices for securing data, and electronic health data in particular, and have made their work available at no cost online from as early as 1997. Organizations that have provided this information included the National Research Council (NRC) and the National Institute of Standards and Technology (NIST). (Hill, Tr. 132-34; CX0740 (Hill Report) ¶ 60).

Response to Finding No. 1122

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> "These guidelines are for use by **Federal organizations** which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

1123. These resources cover topics such as authenticating users, employing access control mechanisms to restrict access to data based on an individual's role, limiting a user's ability to install software, assessing risks and vulnerabilities, encrypting stored data and data in transit, logging access to data and system components, ensuring system and data integrity, protecting network gateways, and maintaining up-to-date software. (Hill, Tr. 135-36; CX0740 (Hill Report) ¶ 60).

Response to Finding No. 1123

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> "These guidelines are for use by **Federal organizations** which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

1124. LabMD could have used these resources to develop a comprehensive information security plan at only the cost of time expended by IT personnel. (Hill, Tr. 136; CX0740 (Hill Report) ¶¶ 60 & n.8, 62).

Response to Finding No. 1124

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered

Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST rather than HIPAA for identifying risks, assessing risks and taking steps to reduce risks, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

1125. Intentionally left blank.

1126. Intentionally left blank.

5.3 Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities

1127. LabMD could have used readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network at relatively low cost. (Hill, Tr. 161-63); CX0740 (Hill Report) ¶¶ 71, 77).

<u>Response to Finding No. 1127</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1128. Intentionally left blank.

5.3.1 Firewalls

1129. When the practice was finally implemented in 2010, review of a monthly firewall log took a LabMD IT employee a maximum of ten minutes. (CX0727-A (Parr, Dep. at 100-01)).

<u>Response to Finding No. 1129</u>

Respondent has no specific response.

1130. LabMD could have used a free mechanism, Wireshark, to do packet level analysis to provide information to determine if Personal Information left the network without authorization, but did not do so. (CX0740 (Hill Report) ¶¶ 68(b), 71).

Response to Finding No. 1130

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1131. On August 25, 2004, Microsoft released Windows XP Service Pack 2, which included Windows Firewall, which LabMD could have deployed on employee workstations at no cost. (CX0740 (Hill Report) ¶ 104(f)).

Response to Finding No. 1131

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it is hearsay.

1132. Intentionally left blank.

1133. Intentionally left blank.

5.3.2 Intrusion Detection System

1134. LabMD could have implemented SNORT, a well-respected and widely used IDS, which has been available at no cost since 1998. (CX0740 (Hill Report) ¶¶ 69 n.22, 104(h)).

Response to Finding No. 1134

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1135. Intentionally left blank.

5.3.3 File Integrity Monitoring

1136. Free file integrity monitoring products, such as Stealth and OSSEC, were available to LabMD during the Relevant Time Period. (CX0740 (Hill Report) ¶ 69 n.22).

Response to Finding No. 1136

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1137. Intentionally left blank.

5.3.4 Penetration Testing

1138. LabMD could have conducted vulnerability scans, or had vulnerability scans conducted for it, throughout the Relevant Time Period at no or low cost, and doing so would have allowed it to correct significant risks much sooner. (CX0740 (Hill Report) ¶ 71).

Response to Finding No. 1138

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1139. Intentionally left blank.

5.3.4.1 Penetration Testing Tools Were Readily Available To LabMD Years Before It Began Penetration Testing

1140. Since 1997, several well-respected and free penetration test and network analysis mechanisms have been available. Examples include Wireshark (released 1998 under a different name), Nessus (free until 2008), and nmap (released 1997). (Hill, Tr. 162; CX0740 (Hill Report) ¶ 71). Those products could have helped the company identify vulnerabilities and correct significant risks. (Hill, Tr. 137-40; CX0740 (Hill Report) ¶¶ 70-71).

Response to Finding No. 1140

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1141. For example, a penetration test of all IP addresses on the network would have identified vulnerabilities such as outdated software, security patches that had not been applied, and administrative accounts with default settings. (Hill, Tr. 139-40; CX0740 (Hill Report) ¶ 70).

Response to Finding No. 1141

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1142. Furthermore, penetration tests also could have identified all open ports within the network and all computers that accepted connection requests; using this information, Respondent could have configured its firewalls to close unneeded ports and to deny connection requests not needed for business purposes. (Hill, Tr. 139; CX0740 (Hill Report) ¶ 70).

<u>Response to Finding No. 1142</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1143. Intentionally left blank.

1144. Intentionally left blank.

5.3.4.2 Penetration Tests Were Low Cost

1145. When LabMD hired an outside IT service provider, ProviDyn, to conduct nine penetration tests in May 2010, the cost was $450. (CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4; CX0048 (ProviDyn Invoice 2172); CX0488 (ProviDyn 2010 Signed Service Solutions Proposal) at 4).

<u>Response to Finding No. 1145</u>

Respondent has no specific response.

1146. Remediating the problems identified by the ProviDyn scans could also have been accomplished at low or no cost. For example, one of the vulnerabilities identified in ProviDyn's April 2010 external vulnerability scan – a Level 5 anonymous FTP problem – could have been remediated at low cost using only IT-employee time to disallow anonymous log-ins. (CX0740 (Hill Report) ¶¶ 72-77; *see supra* § 5.3.4.3.1.1 (The Mapper Server Had an Anonymous FTP Vulnerability that Could Allow Export of All Data on the Server) (¶¶ 759-771).

<u>Response to Finding No. 1146</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact to the extent it suggests that information was sent or received through any means other than a secure file transfer protocol (SFTP). (Fisk, Tr. 1169-1170); (CX0717 (Howard, Dep. at 35, 36, 37, 54); (CX0711 (Dooley, Dep. at 132); (CX0724 (Maire, Dep. at 41); (CX0730 (Simmons, Dep. at 61, 128); (CX0725-A (Martin, Dep. at 60)).

1147. Intentionally left blank.

1148. Intentionally left blank.

5.4 Access Controls for Personal Information

1149. LabMD could have limited employees' access to Personal Information to only the types of Personal Information that the employees needed to perform their jobs at relatively low cost. (Hill, Tr. 166-67; CX0740 (Hill Report) ¶ 85).

Response to Finding No. 1149

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1150. LabMD could have instituted at low cost access control mechanisms and specified policies to limit its employees' access to Personal Information to only the types of Personal Information that those employees needed to perform their jobs. (CX0740 (Hill Report) ¶ 85).

Response to Finding No. 1150

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1151. Because operating systems and applications already have access controls embedded in them, rectifying this issue would have required only the time of trained IT staff and could have been done at relatively low cost. (Hill, Tr. 166-67; CX0740 (Hill Report) ¶ 85).

Response to Finding No. 1151

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1152. LabMD could have regularly purged the Personal Information of the consumers for whom it never performed testing at relatively low cost because this step would have required only the time of trained IT staff. (Hill, Tr. 164; CX0740 (Hill Report) ¶ 80(b)).

Response to Finding No. 1152

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1153. With respect to the Personal Information that LabMD collected from consumers for whom it never performed testing, LabMD could have purged this data through its database applications. (Hill, Tr. 164; CX0740 (Hill Report) ¶ 80(b)).

Response to Finding No. 1153

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1154. IT practitioners regularly purged data from a network throughout the Relevant Time Period. (CX0740 (Hill Report) ¶ 80(b)).

Response to Finding No. 1154

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1155. Intentionally left blank.

1156. Intentionally left blank.

5.5 Training Employees to Safeguard Personal Information

1157. The user is the weakest link in any information security program – a flawless security mechanism can be rendered ineffective by an untrained user. (Hill, Tr. 167-69; CX0740 (Hill Report) ¶ 87).

Response to Finding No. 1157

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1158. An organization should train its employees on how to use any security mechanism that requires employee action, and on any security mechanisms that employees are not prevented from reconfiguring or misconfiguring, such as a firewall on a workstation computer. (Hill, Tr. 168-70; CX0740 (Hill Report) ¶ 87).

Response to Finding No. 1158

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1159. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost. (Hill, Tr. 173-76; CX0740 (Hill Report) ¶ 92).

Response to Finding No. 1159

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1160. Several nationally recognized organizations provide low-cost and free IT security training courses. (Hill, Tr. 173-74; CX0740 (Hill Report) ¶ 89 & n.30).

Response to Finding No. 1160

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1161. For example, the Center for Information Security Awareness, which was established in 2007, provides free security training for individuals and businesses with less than 25 employees. The SysAdmin Audit Network Security Institute, formed in 1989, provides free security training webcasts. Additional free resources can be found online and the Computer Emergency Response Team (CERT) at

Carnegie Mellon University offers e-learning courses for IT professionals for as low as $850. (Hill, Tr. 174-75; CX0740 (Hill Report) ¶ 89 n.30).

Response to Finding No. 1161

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1162. Had LabMD availed itself of the free training materials available, providing employee training on safeguarding information would have required only the expenditure of time by LabMD staff. (Hill, Tr. 173-76).

Response to Finding No. 1162

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it mischaracterizes the record. While Dr. Hill's trial testimony on pages 173 -176 states that LabMD could have availed itself to free training materials, it does not mention that "providing employee training on safeguarding information would have required only the expenditure of time by LabMD staff."

1163. Intentionally left blank.

1164. Intentionally left blank.

5.6 Authentication-Related Security Measures

1165. LabMD could have implemented strong authentication-related security measures at low or no cost. (Hill, Tr. 188; CX0740 (Hill Report) ¶ 96).

Response to Finding No. 1165

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1166. For example, the Windows operating system that LabMD used had as an included feature a centralized password management scheme, which LabMD did not employ. (*Supra* § 5.6.2 (LabMD Did Not Have Enforcement Mechanisms to Ensure Its Employees Used Reasonable Password Practices) (¶¶ 937-938); Hill, Tr. 188; CX0740 (Hill Report) ¶ 95(a) & n.42)

Response to Finding No. 1166

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1167. Using this included feature would not have imposed additional cost to enable LabMD to effect reasonable passwords policies, such as requiring password complexity and forcing password changes. (Hill, Tr. 188).

Response to Finding No. 1167

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1168. Intentionally left blank.

1169. Intentionally left blank.

5.7 Maintain and Update Operating Systems and Other Devices

1170. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost. (Hill, Tr. 194; CX0740 (Hill Report) ¶ 101).

<u>Response to Finding No. 1170</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1171. To limit hackers' ability to exploit software bugs to gain unauthorized access to computer resources and data, IT practitioners should connect to product notification systems and immediately apply remediation processes and updates for vulnerabilities identified. (CX0740 (Hill Report) ¶ 99).

<u>Response to Finding No. 1171</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1172. These systems provide free notifications from vendors, as well as CERT, OSVDB, NIST, and others. (CX0740 (Hill Report) ¶ 99).

Response to Finding No. 1172

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact to the extent it suggests that LabMD, a Covered Entity as that term is defined by HIPAA, should have known that it would be held to the standards identified by NIST regarding implementation of the HIPAA Security Rule, when NIST clearly states:

> "These guidelines are for use by Federal organizations which process sensitive information. The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis."

(CX0400 (NIST Risk Management Guide For Information Technology Systems (SP 800-30) July 2002 at 1)).

1173. Vendors such as Microsoft issue updates and patches to fix coding errors found in their software. (Hill, Tr. 105-06).

Response to Finding No. 1173

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1174. LabMD servers ran software with vulnerabilities that had been identified, reported by the security and IT community, and for which patches were available several years prior to being detected on LabMD computers. (CX0740 (Hill Report) ¶ 100(a)).

Response to Finding No. 1174

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1175. For example, LabMD could have applied software updates or updated the software on hardware devices such as routers and firewalls. (*See* CX0740 (Hill Report) ¶ 100(b) (noting that LabMD had no policy for updating the software on hardware devices such as firewalls and routers)).

Response to Finding No. 1175

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1176. Further, LabMD's LabNet server was configured with a default administrative password, a vulnerability with an urgent risk rating indicating that an attacker could compromise the entire host. (*Supra* § 5.7.1.1.1 (The Veritas Backup Application Was Configured With the Default Administrative Password) (¶¶ 1017-1021)). This problem was detected on LabNet in 2010, even though a solution was available at no cost as early as August 15, 2005. (CX0740 (Hill Report) ¶ 100(d); Hill, Tr. 193- 94).

Response to Finding No. 1176

Respondent objects to the statement that "LabMD's LabNet server was configured with a default administrative password, a vulnerability with an urgent risk rating indicating that an attacker could compromise the entire host" because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.) Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1177. Fixes for vulnerabilities of the Veritas Backup software that were detected by LabMD in 2010 had been made available in 2005 (stop use of default administrative password) and 2007 (fix vulnerability to a buffer overflow attack) by the distributor of the software as no-cost patches. (Hill, Tr. 193-94; CX0740 (Hill Report) ¶ 100(d)).

<u>Response to Finding No. 1177</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1178. Intentionally left blank.

1179. Intentionally left blank.

5.8 Prevent or Detect Unauthorized Access to Personal Information

1180. LabMD could have employed readily available measures to prevent or detect unauthorized access to Personal Information on its computer network at relatively low cost. (Hill, Tr. 201-02; CX0740 (Hill Report) ¶ 106).

Response to Finding No. 1180

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1181. For example, the Windows operating system used by LabMD allowed for, as a standard feature, giving employees non-administrative accounts on workstations to prevent them from installing software. This is a cost-free measure. (Hill, Tr. 202; CX0740 (Hill Report) ¶ 104(a)).

Response to Finding No. 1181

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1182. Further, backups of Personal Information should be stored on devices that are isolated from other employee activities because an employee's workflow may inadvertently expose sensitive information to malicious software, unauthorized software, unauthorized individuals, or unauthorized changes. Storing backups of Personal Information on devices isolated from other employee activates could be cost-free, if an existing device is designated for storage purposes only. (Hill, Tr. 202; CX0740 (Hill Report) ¶ 104(b)).

Response to Finding No. 1182

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS

250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1183. Moreover, LabMD had several firewalls that were not configured to prevent unauthorized traffic from entering the network. (*Supra* § 5.8.3.2 (LabMD Did Not Properly Configure Its Firewall to Block IP Addresses and Unnecessary Ports) (¶¶ 1094-1105). LabMD's existing firewalls, including the Windows software firewall included in the operating system, required only proper configuration at no additional cost. (CX0740 (Hill Report) ¶ 104(f)).

Response to Finding No. 1183

Respondent objects to the statement that "LabMD had several firewalls that were not configured to prevent unauthorized traffic from entering the network: because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel misstates the record. Paragraph 104(f) of Dr. Hills' report does not support Complaint Counsel's statement that "LabMD's existing firewalls….required only proper configuration at no additional cost." Moreover, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1184. Free versions of File Integrity Monitors (FIM), such as Stealth and OSSEC, take snapshots of the systems and compare later snapshots to earlier ones to ensure nothing has changed in the system. Any change may indicate malicious activity, and a FIM can be used to determine the presence of unauthorized software on a system. (Hill, Tr. 202; CX0740 (Hill Report) ¶ 104(h)).

Response to Finding No. 1184

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1185. Other ways an organization can manage or control the inadvertent disclosure of sensitive Personal Information include: eliminating the use of P2P software within the organization; encrypting sensitive information; disabling technologies that allow the transfer of information on devices, such as removing the ports on a laptop; and segregating sensitive and non-sensitive information. (CX0721 (Johnson, Dep. at 116-17)).

Response to Finding No. 1185

Respondent objects to this proposed finding of fact because it is an opinion or conclusion, and not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on ways to control inadvertent disclosure of sensitive PI should be given very little if any weight.

1186. Intentionally left blank.

1187. Intentionally left blank.

6. Peer-to-Peer File Sharing Applications

6.1 Operation of Peer-to-Peer File-Sharing Applications

6.1.1 Overview of Peer-to-Peer Networks

1188. A user looking for information on the Internet must perform a search to find which computer contains that information. (Shields, Tr. 824).

Response to Finding No. 1188

Respondent has no specific response.

1189. The client-server model, which is used in web search engines, is based on specialized servers that exist to answer queries from simpler clients. (CX0738 (Shields Rebuttal Report) ¶ 15). In a client-server network, if the search engine becomes unavailable then searches cannot be conducted. (Shields, Tr. 825-26).

Response to Finding No. 1189

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1190. Peer-to-peer networks are designed to eliminate this single point of failure in a network for finding and sharing files. (Shields, Tr. 826).

Response to Finding No. 1190

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1191. Peer-to-peer networks are often used to share music, videos, pictures, and other materials. (CX0738 (Shields Rebuttal Report) ¶ 14; Ans. ¶ 13; CX0740 (Hill Report) ¶ 42).

Response to Finding No. 1191

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1192. As opposed to the client-server model, a peer-to-peer network allows users to search the computers of other users. (Shields, Tr. 826; CX0738 (Shields Rebuttal Report) ¶¶ 15, 18).

Response to Finding No. 1192

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1193. Peer-to-peer networks make available files that others can come and take. (CX0738 (Shields Rebuttal Report) ¶ 22).

Response to Finding No. 1193

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1194. Intentionally left blank.

1195. Intentionally left blank.

6.1.2 The Gnutella Network

1196. There are many different peer-to-peer networks. (Shields, Tr. 830-31). The network involved in this case is the Gnutella network. (Shields, Tr. 826).

Response to Finding No. 1196

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1197. A user accesses the Gnutella network by using a Gnutella client. Gnutella clients are easy to use and do not require any special expertise. (Shields, Tr. 849).

Response to Finding No. 1197

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1198. At any given time, the Gnutella network could have 2 to 5 million users online. (Shields, Tr. 833; CX0738 (Shields Rebuttal Report) ¶ 60; Fisk, Tr. 1181; RX533 (Expert Report of Adam Fisk) at 15).

Response to Finding No. 1198

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1199. The Gnutella network consists of all the computers, commonly called peers, that are running a program to communicate over the Internet using the Gnutella protocol. (Shields, Tr. 828; CX0738 (Shields Rebuttal Report) ¶ 15; RX533 (Expert Report of Adam Fisk) at 9).

Response to Finding No. 1199

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1200. A protocol functions as a language, specifying what messages can be sent between connected computers, the format of those messages, and the proper responses to those messages. (Shields, Tr. 828).

Response to Finding No. 1200

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1201. A peer is a computer that is connected to the peer-to-peer network using a Gnutella client. (Shields, Tr. 827).

Response to Finding No. 1201

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1202. It is common for peers to join and leave the network often, as the computer is shut down or the client is not running. (CX0738 (Shields Rebuttal Report) ¶ 16).

<u>Response to Finding No. 1202</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1203. Intentionally left blank.

1204. Intentionally left blank.

6.1.2.1 The LimeWire Client

1205. A Gnutella client is a piece of software that understands the Gnutella protocol and allows the peer to interact with other peers using the Gnutella protocol. (Shields, Tr. 827).

<u>Response to Finding No. 1205</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1206. There are several different kinds of Gnutella clients. (CX0738 (Shields Rebuttal Report) ¶ 13; RX533 (Expert Report of Adam Fisk) at 9). The client at issue in this case is LimeWire. (*Infra* § 8.1.2 (1718 File Shared on Gnutella Network Through LimeWire on a LabMD Billing Computer) (¶¶ 1363-1372); CX0738 (Shields Rebuttal Report) ¶ 13).

<u>Response to Finding No. 1206</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1207. LimeWire was a popular Gnutella client. (Shields, Tr. 850).

<u>Response to Finding No. 1207</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1208. LimeWire was used by a wide variety of users to download and share files, including movies, music, software, documents, and text files. (Shields, Tr. 851).

<u>Response to Finding No. 1208</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1209. Intentionally left blank.

1210. Intentionally left blank.

6.1.2.2 File Sharing on Gnutella

1211. A user shares files on the Gnutella network by designating a directory on his or her computer as a shared directory. (Shields, Tr. 828, 852; CX0738 (Shields Rebuttal Report) ¶ 17; CX0740 (Hill Report) ¶ 42). This is typically done when the client is installed and requires the user to select a directory or set of directories on their computer to share. (CX0738 (Shields Rebuttal Report) ¶ 17; Shields, Tr. 829, 852).

Response to Finding No. 1211

Respondent objects to this proposed finding of fact because it contains expert opinion or conclusion, and thus is not a statement of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1212. It is possible for a user to misconfigure a client to designate a shared folder that contains documents and files that the user does not intend to share. (Shields, Tr. 836-37; CX0738 (Shields Rebuttal Report) ¶ 39).

Response to Finding No. 1212

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1213. Once a directory has been selected to be shared, all files within the directory are made freely available for downloading by other users of the Gnutella network. (Shields, Tr. 828-29; CX0738 (Shields Rebuttal Report) ¶ 17; RX533 (Expert Report of Adam Fisk) at 10).

Response to Finding No. 1213

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Both Shields and Fisk testified at the Hearing that "sharing" means the file was "available".

> "I'll note that "sharing" does not mean the files are necessarily downloaded, just that they were available, and that downloading may or may not happen at some point after they are made available through sharing."
>
> (Shields, Tr. 828-829).
>
> Q. And LimeWire allows a user to select a folder, the contents of which will be available for sharing to other LimeWire or P2P applications users on the network; correct?
>
> A. That's correct.
>
> (Fisk Tr. 1181).

1214. The peer must be online and connected to the Gnutella network to share files. (Shields, Tr. 915-16; RX533 (Expert Report of Adam Fisk) at 15).

Response to Finding No. 1214

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1215. Downloading is transferring a file from one computer to another. (Shields, Tr. 829).

Response to Finding No. 1215

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1216. Users looking for a file to download from the Gnutella network will typically enter search terms related to the file, including the file name, and receive a list of possible matches. (CX0738 (Shields Rebuttal Report) ¶ 18; RX533 (Fisk Report) at 11).

Response to Finding No. 1216

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1217. The user then chooses a file they want to download from the list. (CX0738 (Shields Rebuttal Report) ¶ 18). This file is then downloaded from other peers who possess that file. (CX0738 (Shields Rebuttal Report) ¶ 18).

Response to Finding No. 1217

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1218. If many peers have a copy of the file, it is common to download small pieces of the file from many different peers and reassemble the pieces. (CX0738 (Shields

Rebuttal Report) ¶ 18). This speeds file transfer by allowing use of the resources of many peers simultaneously. (CX0738 (Shields Rebuttal Report) ¶ 18).

Response to Finding No. 1218

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1219. The downloading peer is able to verify that it received the file correctly because the search results that are returned include a cryptographic hash of the file. (CX0738 (Shields Rebuttal Report) ¶ 19).

Response to Finding No. 1219

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1220. A hash is a long number computed based on all the data that makes up the file and is statistically unique to that file and is essentially impossible to forge. (CX0738 (Shields Rebuttal Report) ¶ 19).

Response to Finding No. 1220

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1221. A peer can compute the hash of the file when it is assembled and verify that the overall download is correct. (CX0738 (Shields Rebuttal Report) ¶ 19).

Response to Finding No. 1221

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1222. Intentionally left blank.

1223. Intentionally left blank.

6.1.2.3 Shared Files are Difficult or Impossible to Remove from the Network

1224. On the Gnutella network, it is common, though not required, for the folder that receives downloaded files from the network to also be the folder that is designated as the shared directory. (CX0738 (Shields Rebuttal Report) ¶ 20; Fisk, Tr. 1203-04). LimeWire's default setting was to download files to the shared folder. (Fisk, Tr. 1203-04).

Response to Finding No. 1224

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1225. Files downloaded into the shared directory then become available for others to download. (CX0738 (Shields Rebuttal Report) ¶ 20; Fisk, Tr. 1204-05; CX0721 (Johnson, Dep. at 120-21)).

Response to Finding No. 1225

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1226. Once a peer downloads a file from the Gnutella network, the file can be shared by that computer without downloading it again from the original computer. (Shields, Tr. 852-53; CX0738 (Shields Rebuttal Report) ¶ 21; CX0721 (Johnson, Dep. at 99)).

Response to Finding No. 1226

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on file sharing on the Gnutella network should be given very little if any weight.

1227. Files that have been shared on a P2P network are "often viewed and used by others who then re-share them." (CX0721 (Johnson, Dep. at 100)). As they are re-shared, copies of the files appear on different users' accounts on P2P networks. (CX0721 (Johnson, Dep. at 100)).

Response to Finding No. 1227

Respondent objects to this proposed finding of fact because it is an opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on file sharing on the Gnutella network should be given very little if any weight.

1228. Multiplying copies and multiplying users sharing them increases the likelihood that a sensitive file will be misused. (CX0721 (Johnson, Dep. at 100)).

<u>Response to Finding No. 1228</u>

Respondent objects to this proposed finding of fact because it is an opinion. Furthermore, Johnson was not offered as an expert, and thus his ideas on file sharing should be given very little, if any, weight.

1229. Once a file has been shared it can be difficult or impossible to remove it from the network. (Shields, Tr. 853-54; CX0738 (Shields Rebuttal Report) ¶ 21; CX0740 (Hill Report) ¶ 44).

<u>Response to Finding No. 1229</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1230. One reason it is difficult to remove a file from the Gnutella network is that a computer sharing a file may leave and rejoin the network at different times, making it difficult to identify all peers that contain the file. (Shields, Tr. 853; CX0738 (Shields Rebuttal Report) ¶ 16).

<u>Response to Finding No. 1230</u>

Respondent has no specific response.

1231. The Gnutella protocol has no mechanism to retrieve shared files or to prevent further sharing of shared files. (Shields, Tr. 853-54; Fisk, Tr. 1207-08).

<u>Response to Finding No. 1231</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1232. Intentionally left blank.

1233. Intentionally left blank.

6.1.2.4 Firewalls Do Not Prevent Sharing on the Gnutella Network

1234. Files can be downloaded from a peer, even if the peer is behind a firewall. (Shields, Tr. 838-41; Fisk, Tr. 1145-47).

<u>Response to Finding No. 1234</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1235. Firewalls block incoming communications but do not block outgoing communications. (Shields, Tr. 840; Fisk, Tr. 1138-39; RX533 (Expert Report of Adam Fisk) at 8).

<u>Response to Finding No. 1235</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to this proposed finding of fact because it misstates the record- firewalls can block outgoing communications. Mr. Shields stated that "…firewalls **generally** block incoming connections and not outgoing ones…" (Shields, Tr. 840) (emphasis added). Moreover, Mr. Fisk stated that "[f]irewall configurators can choose to configure firewalls to also block outgoing connections…" (RX533 (Expert Report of Adam Fisk, at 8)).

1236. In order to bypass the firewall, communications are sent to the peer behind the firewall through an ultrapeer with which the firewalled peer has already established a connection. (Shields, Tr. 839; Fisk, Tr. 1145-47). This ultrapeer acts as a proxy for the firewalled peer and receives any download requests on behalf of the firewalled peer. (Shields, Tr. 840).

Response to Finding No. 1236

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1237. A request for download sent via an ultrapeer to a peer behind a firewall is sent in the form of a push request. (Shields, Tr. 840). When the peer receives a push request, it contacts the requesting peer through the firewall and uploads the file to the requesting peer. (Shields, Tr. 840).

Response to Finding No. 1237

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1238. Intentionally left blank.

1239. Intentionally left blank.

6.1.3 There are Many Ways to Find Files on the Gnutella Network

6.1.3.1 The Search Function

6.1.3.1.1 Search Using Ultrapeers

1240. In the original Gnutella network, each peer participated in receiving and forwarding search queries. (CX0738 (Shields Rebuttal Report) ¶ 23).

Response to Finding No. 1240

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1241. This system worked well when the network was small, but did not scale well. (CX0738 (Shields Rebuttal Report) ¶ 25). As more users joined the Gnutella network, the overall number of requests grew too large for the system to cope with effectively. (CX0738 (Shields Rebuttal Report) ¶ 25).

Response to Finding No. 1241

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1242. In 2001, the search system changed to a protocol defined in the Gnutella 0.6 definition. (CX0738 (Shields Rebuttal Report) ¶ 25).

Response to Finding No. 1242

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1243. In this system, a small subset of peers that had generally better network connectivity and computing power were promoted to "ultrapeers." (Shields, Tr. 827; CX0738 (Shields Rebuttal Report) ¶ 25).

Response to Finding No. 1243

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1244. Ultrapeers are connected to a larger number of other ultrapeers. (CX0738 (Shields Rebuttal Report) ¶ 25).

Response to Finding No. 1244

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1245. Each normal peer connects to a few ultrapeers, and upon doing so tells each ultrapeer what files it has available for download. (Shields, Tr. 830-31; CX0738 (Shields Rebuttal Report) ¶ 25).

Response to Finding No. 1245

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1246. A peer becomes an ultrapeer if its client detects that it meets the requirements of an ultrapeer, such as network speed and proper operating system. (Shields, Tr. 909-10; Fisk, Tr. 1143). A peer with a firewall cannot be an ultrapeer. (Shields, Tr. 909; Fisk, Tr. 1142).

Response to Finding No. 1246

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1247. A peer is normally connected to about three ultrapeers. (Shields, Tr. 832).

Response to Finding No. 1247

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1248. When a user wants to search, the user makes a search request in the client as before, but instead of the request being forwarded through other peers, it is made to the few ultrapeers to which the peer is connected. (Shields, Tr. 832; CX0738 (Shields Rebuttal Report) ¶ 26). These ultrapeers forward the request to their larger set of ultrapeers. (Shields, Tr. 832-33; CX0738 (Shields Rebuttal Report) ¶ 26).

<u>Response to Finding No. 1248</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1249. Each ultrapeer will contact 32 other ultrapeers. (Shields, Tr. 833). Those ultrapeers will then send it on to other ultrapeers. (Shields, Tr. 833).

<u>Response to Finding No. 1249</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1250. The query will be forwarded for only a limited number of hops. (Shields, Tr. 846-47).

<u>Response to Finding No. 1250</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1251. The number of hops is determined by the time-to-live field (“TTL field”) on the query. (Shields, Tr. 846-47). The TTL field is set to 3 by default. (Shields, Tr. 847).

Response to Finding No. 1251

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1252. Each time the query is forwarded the TTL field is reduced by one. (Shields, Tr. 847). When it reaches zero the query is no longer forwarded. (Shields, Tr. 847).

Response to Finding No. 1252

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1253. The TTL field mechanism was designed to prevent queries from taking over the Gnutella network. (Shields, Tr. 846-47).

Response to Finding No. 1253

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1254. When an ultrapeer receives a query that matches the file index it received from one of its peers, the ultrapeer forwards a query to that peer. (Shields, Tr. 833-34).

Response to Finding No. 1254

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1255. In some versions of the Gnutella protocol, when a sharing peer receives a query from an ultrapeer that matches one of its files, the sharing peer contacts the querying ultrapeer directly to provide information about the file. (Shields, Tr. 834).

Response to Finding No. 1255

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1256. In other versions of the Gnutella protocol, a peer receiving a query from an ultrapeer responds to the querying user by sending the information about the file through the same path that the query arrived, using the ultrapeers to reach the querying computer. (Shields, Tr. 834).

Response to Finding No. 1256

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1257. Intentionally left blank.

1258. Intentionally left blank.

6.1.3.1.2 Searches May Sometimes Fail to Find Files that are on the Gnutella Network

1259. There are many cases in which a search for a particular file might not identify any matches even though the file exists in the network. (CX0738 (Shields Rebuttal Report) ¶ 27; CX0721 (Johnson, Dep. at 101-02)).

Response to Finding No. 1259

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on file sharing should be given very little weight, if any.

1260. During times of high use, network congestion can lead to search requests going unfulfilled due to lack of capacity. (Shields, Tr. 847-48; CX0738 (Shields Rebuttal Report) ¶ 27). Ultrapeers have a limited capability to receive queries and forward them on. (Shields, Tr. 847-48).

Response to Finding No. 1260

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1261. If an ultrapeer receives more queries than it has the ability to receive then some of the queries will be ignored. (Shields, Tr. 847-48). When some ultrapeers involved in a query ignore a request, other ultrapeers may not be at full capacity and will be able to receive and forward the request. (Shields, Tr. 848).

Response to Finding No. 1261

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1262. A file cannot be found on a P2P network if the computer on which the file is located is not connected to the network or running a file-sharing application. (Shields, Tr. 915; CX0721 (Johnson, Dep. at 102, 121); CX0725-A (Martin Dep. at 148)).

Response to Finding No. 1262

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson and Martin were not offered as experts, and thus their ideas on file sharing should be given very little weight, if any.

1263. Peers that contain responsive files might leave the network temporarily, either if the machine is shut down or the Gnutella client is stopped. (CX0738 (Shields Rebuttal Report) ¶ 27; CX0721 (Johnson, Dep. at 100-01)).

Response to Finding No. 1263

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on file sharing should be given very little weight, if any.

1264. Searches also cover only a portion of the network. (Shields, Tr. 847; CX0738 (Shields Rebuttal Report) ¶ 27).

Response to Finding No. 1264

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1265. A peer might be connected to ultrapeers that are connected only to ultrapeers that have no information about the file requested, even if it exists elsewhere on the network. (CX0738 (Shields Rebuttal Report) ¶ 27; CX0721 (Johnson, Dep. at 101-02)). The search would fail in this case, but would succeed if conducted from another portion of the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶ 27).

Response to Finding No. 1265

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson was not offered as an expert, and thus his ideas on file sharing should be given very little weight, if any.

1266. Searches may also fail to find a particular version of a file on the Gnutella network if there are many copies of that file on the network. (Shields, Tr. 848-49). Once a certain number of results have been received by a query, the query terminates. (Shields, Tr. 848-49).

Response to Finding No. 1266

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1267. Intentionally left blank.

1268. Intentionally left blank.

6.1.3.1.3 Hash Searches

1269. In addition to search terms, LimeWire supports hash search. (CX0738 (Shields Rebuttal Report) ¶ 28). A peer in possession of a file can compute the hash for that file and then submit a search request containing that hash to search for other peers that have the identical file. (CX0738 (Shields Rebuttal Report) ¶ 28).

Response to Finding No. 1269

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1270. Subject to the limits of search described above, the peer would then receive a list of other peers that have the bit-for-bit identical file. (CX0738 (Shields Rebuttal Report) ¶ 28).

Response to Finding No. 1270

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1271. Intentionally left blank.

1272. Intentionally left blank.

6.1.3.1.4 Malicious Users Can Search for Misconfigured Peers to Locate Sensitive Files

1273. In addition to searching for particular files, users of the Gnutella network can also search for peers that have been configured in such a way that inadvertent sharing of sensitive information is likely. (CX0738 (Shields Rebuttal Report) ¶ 65).

<u>Response to Finding No. 1273</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1274. Some users of the peer-to-peer networks seek out sensitive documents that peer-to-peer users did not intend to share. (Shields, Tr. 868; CX0738 (Shields Rebuttal Report) ¶ 65).

<u>Response to Finding No. 1274</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1275. Identity thieves search for files to aggregate large amounts of personal data for use or resale. (Wallace, Tr. 1376-77, 1380-81).

Response to Finding No. 1275

Respondent objects to this proposed finding of fact because it misstates the record. At the offered citations, Mr. Wallace is explaining how Tiversa obtained the 1718 file from LabMD, not that identity thieves search for data to resale.

1276. One method for such users to obtain documents is to identify and exploit misconfigured peers that are likely to expose sensitive information, then download and make use of that information. (Shields, Tr. 868-69; CX0738 (Shields Rebuttal Report) ¶ 65).

Response to Finding No. 1276

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1277. A peer is misconfigured if it has been configured to share a folder that contains files and subfolders that the user did not intend, such as the "My Documents" folder or an entire hard drive. (Shields, Tr. 868).

Response to Finding No. 1277

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1278. The users do not need to have any information about the names of the files they hope to find. (CX0738 (Shields Rebuttal Report) ¶ 65).

Response to Finding No. 1278

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1279. Instead, these users gather information about common files that are placed in particular directories when installed. (CX0738 (Shields Rebuttal Report) ¶ 65). For example, they can search for particular operating system files that appear under the directory C:\windows, or common files installed by applications that are placed in the "My Documents" folder. (CX0738 (Shields Rebuttal Report) ¶ 65).

Response to Finding No. 1279

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1280. Similarly, a misconfigured Windows XP peer that was sharing its C: drive would be easily identifiable by searching for a file named zapotec.bmp, which is a default file included in that version of Windows. (CX0738 (Shields Rebuttal Report) ¶ 65).

Response to Finding No. 1280

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1281. Finding such files would signal a high probability that the LimeWire client on a computer was misconfigured and was currently exposing files that the user did not intend to share. (CX0738 (Shields Rebuttal Report) ¶ 66). A user that located such a computer could then use the browse host function described below to download potentially sensitive files that were being shared. (CX0738 (Shields Rebuttal Report) ¶ 66).

<u>Response to Finding No. 1281</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1282. Intentionally left blank.

1283. Intentionally left blank.

6.1.3.1.5 Users Can Locate Sensitive Documents by Searching for File Extensions that are Likely to Contain Sensitive Information

1284. Users of the Gnutella network could also search for files that are more likely to be sensitive by searching for particular file extensions. (CX0738 (Shields Rebuttal Report) ¶¶ 69-76).

<u>Response to Finding No. 1284</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1285. One method for doing so is to perform a file extension search. (Shields, Tr. 872-73; CX0738 (Shields Rebuttal Report) ¶¶ 71-75; Fisk, Tr. 1156). A file extension search is a search that looks for all files of a certain file type. (Shields, Tr. 872; CX0738 (Shields Rebuttal Report) ¶¶ 71-75).

Response to Finding No. 1285

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1286. For example, a user could search for the file extension ".pdf" to locate files formatted as Adobe Portable Document Format (PDF) files. (CX0738 (Shields Rebuttal Report) ¶ 71). This format is commonly used for documents that contain text and images, but which are not intended to be edited. (CX0738 (Shields Rebuttal Report) ¶ 71).

Response to Finding No. 1286

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Moreover, Respondent objects to this proposed finding of fact because ¶ 71 does not state that "[t]his format is commonly used for documents that contain text and images, but which are not intended to be edited."

1287. A search for the term ".pdf" would return results for files that contain those letters in their file names, including in the file extension. (CX0738 (Shields Rebuttal Report) ¶ 71; Fisk, Tr. 1156). Therefore, subject to the limits of search, as discussed above, a search for ".pdf" would return any PDF file available for sharing on the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶ 71).

Response to Finding No. 1287

Respondent objects to this proposed finding of fact to the extent Complaint Counsel suggests that utilizing the search term ".pdf" would have returned the 1718 File. In analyzing this very issue, Mr. Fisk stated:

> …it would be theoretically possible to find the insurance aging file using a search for 'PDF,' but it would be, you know, like a needle in the haystack or something like that than, especially given that with LabMD's network configuration, that computer was behind a firewall…[s]o the searcher searching for "PDF" in the LabMD case would only find a result for that file if they happened to randomly come across that computer out of these millions of computers out there but also if the searcher itself were not firewalled, which was very – at that point on the Internet and today on the Internet is very rare…

(Fisk, Tr. 1156-1157). Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1288. File extension searches were supported from at least January 1, 2005 until at least July 2010. (Shields, Tr. 872); CX0738 (Shields Rebuttal Report) ¶¶ 73-75).

Response to Finding No. 1288

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1289. Intentionally left blank.

1290. Intentionally left blank.

6.1.3.2 Users Can View and Retrieve All Files Being Shared by a Peer Using the Browse Host Function

1291. In addition to searching, many Gnutella clients, including LimeWire, supported a function called host browsing or simply browsing. (Shields, Tr. 844-45; CX0738 (Shields Rebuttal Report) ¶ 29; RX533 (Expert Report of Adam Fisk) ¶ 29). This method would permit a user to find files on the Gnutella network without searching for the files' names. (Shields, Tr. 844-45; CX0738 (Shields Rebuttal Report) ¶¶ 30-31, 56-58).

<u>Response to Finding No. 1291</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1292. Using this functionality, a peer that was connected to another peer, perhaps while downloading a file as a result of a search, could request a list of other files that the other peer was also making available. (Shields, Tr. 844-45, 867-68; CX0738 (Shields Rebuttal Report) ¶¶ 29-30; Fisk, Tr. 1151, 1182-83; RX533 (Expert Report of Adam Fisk) at 16; Johnson, Tr. 800-01; CX0721 (Johnson, Dep. at 123); Wallace, Tr. 1404).

<u>Response to Finding No. 1292</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Further, Johnson and Wallace were not offered as experts, and thus their ideas on file sharing should be given very little weight, if any.

1293. The outside user could then open and download any of the files in the shared folder without additional searching. (Shields, Tr. 845; CX0738 (Shields Rebuttal Report) ¶ 30; RX533 (Expert Report of Adam Fisk) at 16). The outside user could also open any of the other folders in the sharing folder. (CX0738 (Shields Rebuttal Report) ¶ 30).

Response to Finding No. 1293

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1294. This feature allows a more general approach to discovering files of interest inside the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶ 31). Users can look through shared folders of other users that have collections of files of interest to the user. (CX0738 (Shields Rebuttal Report) ¶ 31; Wallace, Tr. 1372, 1404, 1442).

Response to Finding No. 1294

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1295. If one file of some particular type is identified through search, a user might find it worthwhile to browse the other user's files to see if anything else of interest is available on that computer. (Shields, Tr. 867-70; CX0738 (Shields Rebuttal Report) ¶ 31).

Response to Finding No. 1295

1296. A user could examine the contents of a peer's shared folder using the browse host function even if the peer was behind a firewall, as long as the computer doing the searching is not behind a firewall. (Shields, Tr. 844-45; CX0738 (Shields Rebuttal Report) ¶¶ 62-63; RX533 (Expert Report of Adam Fisk) at 16).

Response to Finding No. 1296

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1297. Intentionally left blank.

1298. Intentionally left blank.

6.1.3.2.1 Creating Custom Software that Uses the Preexisting Search Functions of the Gnutella Network is Relatively Simple

1299. In addition to searching the Gnutella network using an existing Gnutella client, it is also possible, and relatively simple, to create custom software to perform searches using the Gnutella protocol. (CX0738 (Shields Rebuttal Report) ¶¶ 82-91).

Response to Finding No. 1299

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1300. Writing custom search software is not challenging because most of the code required already exists. (CX0738 (Shields Rebuttal Report) ¶ 82). It would be possible for someone with as little as an undergraduate computer science degree and basic networking knowledge to create custom search software. (Shields, Tr. 879-81; CX0738 (Shields Rebuttal Report) ¶ 82).

Response to Finding No. 1300

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1301. It would be relatively easy, for example, to create a piece of software that sought out peers on the Gnutella network and used the browse host function to create an index of the files available on the network. (CX0738 (Shields Rebuttal Report) ¶ 84). Such software is called crawler software. (Shields, Tr. 878).

Response to Finding No. 1301

Respondent objects to this proposed finding of fact because it misstates the record. Mr. Shields did not state that "[i]t would be relatively easy" to create crawler software. Furthermore, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1302. A custom search program developer could use preexisting code to create this software relatively easily. (CX0738 (Shields Rebuttal Report) ¶¶ 86-90). Such code reuse is a common practice among computer programmers. (CX0738 (Shields Rebuttal Report) ¶ 87).

Response to Finding No. 1302

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1303. Use of existing code removes the need to have a complete understanding of all aspects of the Gnutella protocol. (CX0738 (Shields Rebuttal Report) ¶ 90).

Response to Finding No. 1303

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1304. Many programmers have already produced software that creates an index of the contents of the Gnutella network by crawling the network. (CX0738 (Shields Rebuttal Report) ¶¶ 92-93). Several of these developers appear to have done this with little resources. (Shields, Tr. 879-81; CX0738 (Shields Rebuttal Report) ¶ 94).

Response to Finding No. 1304

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1305. Crawling the Gnutella network is a common enough activity that it has its own Wikipedia page. (CX0738 (Shields Rebuttal Report) ¶ 95).

Response to Finding No. 1305

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1306. A developer could easily design crawling software that downloaded files found through crawling without then sharing those files on the Gnutella network. (CX0738 (Shields Rebuttal Report) ¶¶ 97-99).

Response to Finding No. 1306

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1307. Intentionally left blank.

1308. Intentionally left blank.

6.1.4 Risk of Inadvertent Sharing through Peer-to-Peer File Sharing Applications

1309. Using a peer-to-peer client to access a peer-to-peer network creates a significant risk that files on a peer will inadvertently be shared with other users on the network. (*Infra* ¶¶ 1310-1313; Wallace, Tr. 1338).

Response to Finding No. 1309

Respondent objects to this proposed finding of fact because it is unsupported by citations to the record. At page 1338 of the Trial Transcript, Mr. Wallace does not state that using a peer to peer network creates a risk of inadvertent sharing, rather this page discusses the fact that Mr. Wallace was quoted in a news article about "the ability to find and expose data, PII, that is loose on peer-to peer networks." Furthermore, Respondent objects to this proposed finding of fact because it is an opinion or conclusion, and not a finding of fact.

1310. Inadvertent file sharing can occur if a user unintentionally places sensitive or valuable files in the folder of shared files on the computer. (Shields, Tr. 833; CX0738 (Shields Rebuttal Report) ¶¶ 38-39).

Response to Finding No. 1310

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1311. Inadvertent sharing can also occur if the user specifies the wrong folder to share, which may contain files the user did not intend to share. (Shields, Tr. 883; CX0738 (Shields Rebuttal Report) ¶ 15).

Response to Finding No. 1311

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1312. The security risks of peer-to-peer software, including inadvertent file sharing, are well known. (Shields, Tr. 883; CX0738 (Shields Rebuttal Report) ¶ 40; CX0740 (Hill Report) ¶ 44). The risks have been known since the early 2000s. (Shields, Tr. 883-84; CX0738 (Shields Rebuttal Report) ¶ 40).

Response to Finding No. 1312

Respondent objects to this proposed finding of fact because it contains expert opinion or conclusion, and thus is not a statement of fact. *See In re Realcomp II, Ltd.*,2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed or analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1313. Security professionals have known since the early 2000s that peer-to-peer networks create a large security risk, in part because a user could allow sharing of proprietary or confidential corporate documents. (CX0738 (Shields Rebuttal Report) ¶ 45).

Response to Finding No. 1313

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1314. Intentionally left blank.

1315. Intentionally left blank.

6.1.4.1 Warnings Issued by Third Parties

1316. The fact that inadvertent sharing of sensitive documents was a concern and needed to be prevented by specific policy, procedure, and training was well known among information technology practitioners by 2006. (*Infra* §§ 7.1.4.1.1 (The SANS Reading Room) (¶¶ 1318-1327), 7.1.4.1.2 (US-CERT) (¶¶ 1330-1335); Hill, Tr. 120-21).

Response to Finding No. 1316

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); see also at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that infra or supra should also not be used.).

Furthermore Respondent objects to this proposed finding of fact because it misstates Dr. Hill's testimony. Dr. Hill did not say that the inadvertent sharing of sensitive documents "was well known" among information technology practitioners, but only that "[s]ecurity experts have been providing warnings as early as 2005."

Moreover, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1317. Intentionally left blank.

6.1.4.1.1 The SANS Reading Room

1318. SANS is the System Administration, Networking, and Security Institute. (CX0738 (Shields Rebuttal Report) ¶ 40). It is a well-respected organization dedicated to training system administrators who operate and maintain computer systems and networks in the practice of security. (Shields, Tr. 884-85; CX0738 (Shields Rebuttal Report) ¶ 40).

Response to Finding No. 1318

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1319. The SANS Reading Room contains many documents that describe the risks presented by peer-to-peer software. (*Infra* ¶¶ 1320-1327; CX0738 (Shields Rebuttal Report) ¶ 40). These works show computer security professionals were aware that peer-to-peer networks provided a large risk due to the fact that a user could share proprietary or confidential corporate documents. (*Infra* ¶¶ 1320-1327; CX0738 (Shields Rebuttal Report) ¶ 45).

Response to Finding No. 1319

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1320. SANS materials are a prime resource for information technology practitioners. (CX0738 (Shields Rebuttal Report) ¶ 40). Its advanced students produce papers on security topics that are then made publicly available on the SANS website. (Shields, Tr. 885; CX0738 (Shields Rebuttal Report) ¶ 40).

Response to Finding No. 1320

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1321. Many papers from the early 2000s on the SANS website described the risks of peer-to-peer software. (CX0738 (Shields Rebuttal Report) ¶¶ 40-44).

Response to Finding No. 1321

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1322. In a 2002 paper titled "Peer-to-Peer File-Sharing Networks: Security Risks" available on the SANS reading room, William Couch wrote:

"Another real danger of P2P networks is that, although theoretically the user controls what subdirectories he/she makes available to peer users, sometimes more subdirectories are shared than is known or intended."

(CX0874 (SANS Institute InfoSec Reading Room_Peer-to-Peer File-Sharing Networks Security) at 6; Shields, Tr. 885-86; CX0738 (Shields Rebuttal Report) ¶ 41).

Response to Finding No. 1322

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1323. Couch also wrote:

"Therefore, it is up to users, and security administrators, to be aware of the risks implicit in this wide-open architecture. The safest course of action is to not use, or allow, P2P file-sharing software."

(CX0874 (SANS Institute InfoSec Reading Room_Peer-to-Peer File-Sharing Networks Security) at 11; Shields, Tr. 886; CX0738 (Shields Rebuttal Report) ¶ 41).

Response to Finding No. 1323

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1324. In July 2002, another SANS student contributed a paper titled "Security Implications of 'Peer-to-Peer' Software." (CX0875 (Security Implications of "Peer-To-Peer" Software); CX0738 (Shields Rebuttal Report) ¶ 42). In this paper, Choi wrote:

"File sharing applications such as this present multiple exposure opportunities for the enterprise. Issues of intellectual property are paramount. Companies bear some measure of liability for employees trading and storing copyrighted works in the office. Equally distressing is the opportunity for unintentionally sharing proprietary or delicate information through carelessly or improperly configured clients. Allowing documents to be shared without explicit permissions is an easy mistake for the unwary user, and users have been known to unintentionally share entire disc volumes. This 'information leakage' could be the most expensive security issue faced by the enterprise, as it has can have [sic] the greatest legal liability. This is exacerbated when employees install and configure file-sharing software outside a defined security process and infrastructure."

(CX0875 (Security Implications of "Peer-To-Peer" Software) at 4; (CX0738 (Shields Rebuttal Report) ¶ 42).

<u>Response to Finding No. 1324</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1325. In a December 20, 2003 paper titled "Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications," Lucas Ayers wrote:

"It appears most of the sharing of personal files is due to user error – where a user mistakenly shares documents they didn't mean to. While this is not a true technical issue like firewall rule sets or router access lists, it is very much a Security issue. Informing users about security and making everyone aware of the consequences of their actions, is one of the most imports [sic] tasks any security officer has.

"There are also issues with the wizards and setup programs of some of these file sharing applications used during installation. The wizards will ask the user if they want to search for the location of typical files people share. If you happen to have a bunch of music files located in your 'My Documents' folder (this is a typical location people have personal files on their computers), the setup program will share that whole folder with the rest of the P2P network. Not just the music you meant to share, but everything in that folder!"

(CX0876 (Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications) at 14; (CX0738 (Shields Rebuttal Report) ¶ 43).

Response to Finding No. 1325

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1326. In a 2003 paper, titled "Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment," Stephen Farquhar wrote:

"Sharing the File Server in one easy step – Astute users will selectively share files, but many users accept application defaults or blindly tick the first checkbox they see. This can result in the entire contents of their hard drive being shared or worse, all drives including network drives to be shared. Hence, unwittingly, exposing the contents of the corporate file server to the public becomes a minor task."

(CX0877 (Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment) at 8; CX0738 (Shields Rebuttal Report) ¶ 44).

<u>Response to Finding No. 1326</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1327. Farquhar also wrote:

"The task of preventing the use of P2P applications in the corporate environment is a subset of the task of preventing any unauthorized software usage and starts with policy, followed by a variety of techniques to form multi-layered defences."

(CX0877 (Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment) at 15; CX0738 (Shields Rebuttal Report) ¶ 44).

<u>Response to Finding No. 1327</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1328. Intentionally left blank.

1329. Intentionally left blank.

6.1.4.1.2 US-CERT

1330. The knowledge of the security risks posed by peer-to-peer networks was not limited to SANS students. (CX0738 (Shields Rebuttal Report) ¶ 46). By 2005, the US Computer Emergency Readiness Team (US-CERT) had published warnings about the risks of peer-to-peer networks. (CX0738 (Shields Rebuttal Report) ¶ 46).

<u>Response to Finding No. 1330</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1331. US-CERT is a government agency leading efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nations while protecting the constitutional rights of Americans. (Shields, Tr. 886; CX0738 (Shields Rebuttal Report) ¶ 46 n.10).

Response to Finding No. 1331

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1332. US-CERT is known as an expert on security threats and as a resource of information about those threats. (Shields, Tr. 887).

Response to Finding No. 1332

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1333. In 2005, a page of the US-CERT website read:

"**Exposure of sensitive or Personal Information** – By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal

> information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft . . . ."

(CX0878 (US-CERT - Risks of File-Sharing Technology) at 1; Shields, Tr. 887; CX0738 (Shields Rebuttal Report) ¶ 46).

Response to Finding No. 1333

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1334. By 2005, various organizations had warned about the risk of inadvertent file sharing through peer-to-peer programs, and by 2006, concern about peer-to-peer networks and defending against security problems they had caused had reached the state of best practice. (CX0738 (Shields Rebuttal Report) ¶ 47).

Response to Finding No. 1334

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD and other similarly situated business entities who would be expected to comply with the FTC's data security standards would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1335. In the 2006 document, "Security Best Practices," Dr. Eric Cole wrote:

"The organization's security policies should address applications, services and activities that are prohibited. These can include, among others, viewing inappropriate material, spam, peer-to-peer file sharing, instant messaging, unauthorized wireless devises and the use of unencrypted remote connections such as Telnet and FTP."

(CX0879 (Secure Anchor - Security Best Practices at 2); CX0738 (Shields Rebuttal Report) ¶ 47).

<u>Response to Finding No. 1335</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1336. Intentionally left blank.

1337. Intentionally left blank.

6.1.4.2 Warnings Issued by the Commission

1338. By 2003, the FTC had begun warning about the security dangers presented by the use of peer-to-peer software, through publications directed at both consumers and business, as well as testimony before Congress. (*Infra* §§ 7.1.4.2.1 (Consumer Education) (¶¶ 1340-1342), 7.1.4.2.2 (Business Education) (¶ 1345), 7.1.4.2.3 (Other Publications: Staff Report) (¶ 1347), 7.1.4.2.4 (Congressional Testimony) (¶¶ 1349-1351)).

Response to Finding No. 1338

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1339. Intentionally left blank.

6.1.4.2.1 Consumer Education

1340. In 2003, the FTC released a consumer alert warning consumers that use of peer-to-peer software may "unknowingly allow others to copy private files you never intended to share." (CX0770 (FTC Consumer Alert: File-Sharing: A Fair Share? Maybe Not) at 2). The alert also warned that users might "download a virus or facilitate a security breach." (CX0770 (FTC Consumer Alert: File-Sharing: A Fair Share? Maybe Not) at 2).

Response to Finding No. 1340

Respondent objects to the extent this proposed finding of fact suggests that LabMD, and other similarly situated business entities who would be expected to comply with the FTC's data security standards, would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1341. In 2005, the FTC issued another consumer alert discussing the dangers of peer-to-peer software. (CX0778 (Revised FTC Consumer Alert: P2P File-Sharing: Evaluating the Risks). The alert warned consumers that "you could open access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents." CX0778 (Revised FTC Consumer Alert: P2P File-Sharing: Evaluating the Risks) at 2). The alert also discussed the risk that files downloaded from a peer-to-peer network could contain viruses or other unwanted content. (CX0778 (Revised FTC Consumer Alert: P2P File-Sharing: Evaluating the Risks) at 2).

Response to Finding No. 1341

Respondent objects to the extent this proposed finding of fact suggests that LabMD, and other similarly situated business entities who would be expected to comply with the FTC's data security standards, would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1342. Also in 2005, the FTC published a consumer education brochure entitled "Stop. Think. Click: 7 Practices for Safer Computing." (CX0781 (FTC Distribution: Stop.Think.Click: 7 Practices for Safer Computing)). The brochure described the risk of file-sharing software, stating that users could "allow access not just to the files you intend to share, but also to other information on your hard drive, like your tax returns, email messages, medical records, photos, or other personal documents." (CX0781 (FTC Distribution: Stop.Think.Click: 7 Practices for Safer Computing) at 5).

Response to Finding No. 1342

Respondent objects to the extent this proposed finding of fact suggests that LabMD, and other similarly situated business entities who would be expected to comply with the FTC's data security standards, would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1343. Intentionally left blank.

1344. Intentionally left blank.

6.1.4.2.2 Business Education

1345. In 2004, the FTC issued a joint press release with the Counsel of Better Business Bureaus and the National Cyber Security Alliance that offered businesses tips on keeping their computer systems secure. (CX0771 (Press Release: Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure)). The press release warned that file sharing software could "lead to viruses, as well as a competitor's ability to read the files on your computer." (CX0771 (Press Release: Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure) at 2). The press release recommended "prohibiting your employees from installing file-sharing programs on their computers." (CX0771 (Press Release: Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, Offer Businesses Tips For Keeping Their Computer Systems Secure) at 2).

Response to Finding No. 1345

Respondent objects to the extent this proposed finding of fact suggests that LabMD, and other similarly situated business entities who would be expected to comply with the

FTC's data security standards, would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1346. Intentionally left blank.

6.1.4.2.3 Other Publications: Staff Report

1347. In June 2005, FTC staff issued a report on a 2004 workshop about peer-to-peer file sharing technology. (CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report)). The report discussed risks presented by peer-to-peer file sharing software. (CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report) at 13-17). The report stated that several workshop participants noted the risk of inadvertent file-sharing and indicated that software that allowed users to search the shared folders of users created a greater risk. (CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report) at 14). The report also discussed the risks of downloading spyware and viruses. (CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report) at 14-15).

Response to Finding No. 1347

Respondent objects to this proposed finding fact because it is an incomplete summary of the article. Panelists also discussed follow-up research they conducted which suggested that the "risk of inadvertent file sharing may be decreasing..." (CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report) at 14-15). Furthermore, Respondent objects to the extent this proposed finding of fact suggests that LabMD, and other similarly situated business entities who would be expected to comply with the FTC's data security standards, would be required to guard against the dangers of P2P file sharing programs even during a time when the FTC consider such file sharing programs to be no more than a neutral threat. *See 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 Sept. 3, 2015).

1348. Intentionally left blank.

6.1.4.2.4 Congressional Testimony

1349. In May 2004, the FTC offered testimony before House of Representatives' Committee on Energy and Commerce's Subcommittee on Commerce, Trade and Consumer Protection. (CX0773 (Prepared Statement of FTC: Hearing on Online Pornography: Closing the Door on Pervasive Smut)). The testimony concerned online pornography and included a discussion of "the security risks of improperly configuring P2P file-sharing software, including the risk that sensitive personal files inadvertently may be disclosed." (CX0773 (Prepared Statement of FTC: Hearing on Online Pornography: Closing the Door on Pervasive Smut) at 7-8).

Response to Finding No. 1349

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited testimony includes a reference to a consumer alert issued by the FTC in July of 2003. According to the cited testimony, that consumer alert addressed "the security risks of improperly configuring P2P file-sharing software, including the risk that sensitive personal files may inadvertently may be disclosed." The cited exhibit merely cites this consumer alert and does not "discuss" the risks.

1350. In June 2004, the FTC offered testimony before the Senate's Subcommittee on Competition, Infrastructure, and Foreign Commerce of the Committee on Commerce, Science, and Transportation. (CX0775 (Prepared Statement of FTC: Hearing on P2P File-Sharing Technology)). The testimony was part of a hearing on peer-to-peer file-sharing technology and discussed the "significant risks to consumers" created by the technology. (CX0775 (Prepared Statement of FTC: Hearing on P2P File-Sharing Technology) at 4). The testimony warned that peer-to-peer software could result in the downloading of spyware, and that consumers could "inadvertently place files with sensitive personal information in their directory of files to be shared." (CX0775 (Prepared Statement of FTC: Hearing on P2P File-Sharing Technology) at 4).

Response to Finding No. 1350

Respondent has no specific response.

1351. In 2007, the FTC offered testimony concerning peer-to-peer file sharing technology before the House of Representatives' Committee on Oversight and Government Reform. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues)). The testimony addressed the risks created by file sharing technology, including inadvertent sharing and downloading viruses or spyware. (CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 2-3).

Response to Finding No. 1351

Respondent has no specific response.

1352. Intentionally left blank.

1353. Intentionally left blank.

7. Security Incidents at LabMD

7.1 LimeWire Installation and Sharing of 1718 File

7.1.1 The 1718 File

7.1.1.1 Description

1354. The 1718 File is a 1,718 page LabMD insurance aging report with the filename "insuranceaging_6.05.071.pdf" that is identified as the "P2P insurance aging file" in Paragraphs 17, 18, 19, and 21 of the Complaint. (JX0001-A (Joint Stips. of Fact, Law, & Authenticity) at 1); CX0008-0011 (*in camera*), CX0697 (*in camera*) (1718 File).

Response to Finding No. 1354

Respondent has no specific response.

1355. The 1718 File is an example of an insurance aging report. (JX0001-A (Joint Stips. of Fact, Law, & Authenticity) at 1; CX0706 (Brown, Dep. at 51-54)).\

Response to Finding No. 1355

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the Joint Stipulations of Fact, Law & Authenticity. While the cited testimony of Ms. Sandra Brown indicates that the information contained in the 1718 file was information that would typically be contained in an insurance aging report, she did not testify that the 1718 file was "an example of an insurance aging report." In addition, the cited portions of JX0001 do not support Complaint Counsel's purported finding of fact.

1356. The 1718 File was created by or for LabMD. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 9-10, Adm. 47).

Response to Finding No. 1356

Respondent has no specific response.

1357. The 1718 File was created and stored on a LabMD computer. (Daugherty, Tr. 1078-79).

Response to Finding No. 1357

Respondent has no specific response.

1358. The 1718 File is a billing file from the Lytec system. (CX0709 (Daugherty, Dep. at 146); CX0736 (Daugherty, IHT at 83-84)).

Response to Finding No. 1358

Respondent has no specific response.

1359. Intentionally left blank.

1360. Intentionally left blank.

7.1.1.2 Personal Information in 1718 File

1361. The 1718 File contains the Personal Information of approximately 9,300 consumers, including names; dates of birth; Social Security numbers; CPT codes for laboratory tests conducted; and, in some instances, health insurance company names, addresses, and policy numbers. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8, Adm. 37; Ans. ¶ 19; CX0008-0011 (*in camera*), CX0697 (*in camera*) (1718 File)).

<u>Response to Finding No. 1361</u>

Respondent has no specific response.

1362. Intentionally left blank.

7.1.2 1718 File Shared on Gnutella Network Through LimeWire on a LabMD Billing Computer

1363. The Gnutella client LimeWire was downloaded and installed on a computer used by LabMD's billing department manager (the "Billing Computer") in or about 2005. (Ans. ¶ 18(a); CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) at 4, Resp. to Interrog. 3; CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6; CX0150 (Screenshot: C:\) at 1; CX0730 (Simmons, Dep. at 10); CX0709 (Daugherty, Dep. at 144); CX0736 (Daugherty, IHT at 64-65); CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8-9, Adms. 40-41)).

<u>Response to Finding No. 1363</u>

Respondent has no specific response.

1364. Prior to May 2008, LabMD did not detect the installation or use of LimeWire on any LabMD computer. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 9, Adms. 43-46).

<u>Response to Finding No. 1364</u>

Respondent has no specific response.

1365. Before being notified in May 2008 that the 1718 File was available on the P2P network, LabMD did not discover that LimeWire was installed on the Billing Computer. (CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 5-6 (LabMD discovered LimeWire after being contacted regarding 1718 File)).

<u>Response to Finding No. 1365</u>

Respondent has no specific response.

1366. Rosalind Woodson was LabMD's billing department manager in May 2008. (CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6; CX0730 (Simmons, Dep. at 11)).

<u>Response to Finding No. 1366</u>

Respondent has no specific response

1367. A copy of the 1718 File had been maintained on the Billing Computer. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 9, Adm. 42).

Response to Finding No. 1367

Respondent has no specific response

1368. The Billing Computer's entire "My Documents" folder was designated for sharing on LimeWire. (CX0154 (Screenshot: LimeWire Get Started); CX0156 (Screenshot: LimeWire: Options: Shared Folders); CX0730 (Simmons, Dep. at 12, 28-29, 32)).

Response to Finding No. 1368

Respondent has no specific response

1369. The 1718 File was in the "My Documents" folder on the Billing Computer. (CX0710-A (Daugherty, LabMD Designee, Dep. at 200). The "My Documents" folder includes over 900 documents designated for sharing on LimeWire, including the 1718 File. (JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 4, Stip. 11; CX0710-A (Daugherty, LabMD Designee, Dep. at 200); CX0156 (Screenshot: LimeWire: Options: Shared Folders) at 1; CX0730 (Simmons, Dep. at 32))

Response to Finding No. 1369

Respondent has no specific response.

1370. The 1718 File is a copy of a file on the Billing Computer that had LimeWire installed on it. (CX0709 (Daugherty, Dep. at 146-47); CX0710-A (Daugherty, LabMD Designee, Dep. at 32-33)).

Response to Finding No. 1370

Respondent has no specific response.

1371. LabMD had no business need for LimeWire on the Billing Computer. (Ans. ¶ 20; CX0716 (Harris, Dep. at 146)).

Response to Finding No. 1371

Respondent has no specific response

1372. LabMD did not have any security measures in place to detect or prevent P2P sharing from the Billing Computer. (CX0730 (Simmons, Dep. at 13, 54-56); CX0734 (Simmons, IHT at 38-39)).

Response to Finding No. 1372

Respondent objects to the extent that this proposed finding of fact is intended to apply to time periods other than October 2006 through August 2009. Ms. Hudson was employed by LabMD during those times and, as such, her knowledge would be limited to the duration of his employment.

1373. Intentionally left blank.

1374. Intentionally left blank.

7.1.2.1 LabMD Shared Hundreds of Other Files via LimeWire

1375. In addition to sharing the 1718 File, LabMD's Billing Computer was also sharing more than 900 other files on the P2P network through LimeWire. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4; CX0730 (Simmons, Dep. at 33-34); CX0154 (Screenshot: LimeWire Get Started) at 1; CX0152 (Screenshot: LimeWire: My Shared Files) at 1).

Response to Finding No. 1375

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. In JX0001-A, the parties stipulated that "More than 900 files on a computer used by LabMD's billing manager, including the 1718 File, were **available** for sharing through LimeWire." (JX0001-A(Joint Stips. Of Law, Fact, and Authenticity) at 4 (emphasis added). As such, the citation to JX0001 does not support the proposed finding of fact, as worded.

1376. Other documents containing Personal Information, including names, dates of birth, Social Security numbers, and health insurance identification numbers, were contained within the folder designated for sharing, and they were downloaded by a third party using P2P software. (RX645 (*in camera*) (LabMD Documents produced by Wallace) at 39, 42-43; *see also* Wallace, Tr. 1404-07).

Response to Finding No. 1376

Respondent has no specific response

1377. The files also included hundreds of music files, as well as .pdf files with names such as "W-9 Form," "Employee Application Benefits," "LetterHead," and "Medicare Refund Form," and usernames and passwords in a Word document. (CX0152 (Screenshot: LimeWire: My Shared Files) at 1; Wallace, Tr. 1405).

Response to Finding No. 1377

Respondent objects to this proposed finding as it is unsupported by the citations to the record. Neither the cited testimony of Wallace, nor CX0152 indicate the number of files in question.

1378. The warnings that the LimeWire application displayed for the user indicated the Billing Computer was sharing many files and sub-folders. (CX0152 (Screenshot: LimeWire: My Shared Files) at 1; CX0154 (Screenshot: LimeWire Get Started) at 1).

Response to Finding No. 1378

Respondent has no specific response

1379. Such files could have been found by using search terms that could have been of interest to other LimeWire users, including potential identity thieves. (CX0738 (Shields Rebuttal Report) ¶ 58).

Response to Finding No. 1379

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1380. Intentionally left blank.

1381. Intentionally left blank.

7.1.2.2 Use of LimeWire at LabMD Was Well Known Internally

1382. It was known that Ms. Woodson played music on her computer through LimeWire. (CX0716 (Harris, Dep. at 87); *see also* CX0707 (Bureau, Dep. at 94)).

Response to Finding No. 1382

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Not only does the cited testimony of Nicole Harris and Matt

Bureau, CX0716 and CX0707, fail to support the proposed finding of fact, it directly contradicts it. In the cited portion of her deposition, Ms. Harris testified as follows:

> Q. To your knowledge, was it known Ms. Woodson played music on her computer?
>
> A. Yes.
>
> ***Q. To your knowledge, did others within the company know if she was [playing music] through LimeWire?***
>
> ***A. I don't know. I can't recall. Not to my knowledge.***

(CX0716 (Harris, Dep. At 87-88)) (emphasis added).

As to CX0707, the deposition of Matt Bureau, Complaint Counsel again intentionally distorts the record. Mr. Bureau testified as follows:

> Q. Were you familiar with LimeWire when you were at LabMD?
>
> A. Yeah. I knew what it was. Yeah.
>
> Q. When you were at LabMD, were there any discussions regarding LimeWire at LabMD?
>
> A. I think it came up – I want to say that maybe some of the ladies in the billing department might have used it for music or something like that.
>
> Q. How did you find out about LimeWire's use at LabMD?
>
> A. I am going to say John Boyle mentioned a few of them had it on their machine. I don't remember. I am pretty sure – you know, I am trying to even remember if that actually came up or not. I know they listened to music on their computers. But, I mean, I am trying to think did I hear that from a manager or not. I don't remember. I think it was mentioned once before.

> Q. You mentioned that they listened to music –
>
> A. The employees in the billing department.
>
> Q. So not a specific employee but –
>
> A. Right.
>
> Q. But more than one employee listened to music?
>
> A. Yeah.
>
> Q. Do you know whether it was through the radio or through a computer?
>
> A. I know that some was radio and some was through the computer. You know, I think I was just told, yeah, just make sure they don't have applications like LimeWire and stuff like that one there.
>
> ***Q. Did you check the computers to see if people had had LimeWire or any other peer-to-peer file sharing software?***
>
> ***A. Yeah I looked through them. I never saw any of that that I remember.***

(CX0707 (Bureau, Dep. at 94-95)) (emphasis added).

1383. It "was out in the open" that Ms. Woodson downloaded music from LimeWire and Ms. Woodson told others in the billing department that she downloaded music from LimeWire. (CX0716 (Harris, Dep. at 149)).

<u>Response to Finding No. 1383</u>

Respondent objects to this proposed finding of fact as worded because it is unsupported by the citation to the record. Ms. Harris' testimony was "out in the open" to "other people in the billing department." Ms. Harris' testified as follows:

> Q. (By Mr. Mehm) And Ms. Woodson made it pretty clear to you that she was downloading music from Limewire?
>
> A. Yes. She told me.

> Q. Did you hear her telling other people that too?
>
> A. Yes. It was out in the open, so –
>
> ***Q. To who?***
>
> ***A. To other people in the billing department.***
>
> ***Q. And anyone outside?***
>
> ***A. Not to my knowledge, no.***

(CX0716 (Harris, Dep. at 149)) (emphasis Added).

1384. Prior to the 2008 incident, other employees were aware that Ms. Woodson had LimeWire on her workstation. (CX0716 (Harris, Dep. at 86)).

Response to Finding No. 1384

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Ms. Harris simply does not testify to the proposition that Complaint Counsel asserts on Page 86 of her deposition transcript.

1385. Ms. Woodson told Ms. Harris that she downloaded LimeWire. (CX0716 (Harris, Dep. at 88)). Ms. Woodson also told Ms. Harris that she downloaded music from LimeWire. (CX0716 (Harris, Dep. at 149)).

Response to Finding No. 1385

Respondent has no specific response.

1386. Ms. Harris knew that Ms. Woodson installed LimeWire on her work computer because Ms. Woodson listened to music on her work computer, downloaded CDs, and passed out CDs. (CX0716 (Harris, Dep. at 86)).

Response to Finding No. 1386

Respondent has no specific response.

1387. Ms. Woodson created music CDs at LabMD and gave them to other employees. (CX0716 (Harris, Dep. at 89)).

Response to Finding No. 1387

Respondent has no specific response.

1388. Ms. Woodson made the CDs through LimeWire by downloading music to her computer. (CX0716 (Harris, Dep. at 89)).

Response to Finding No. 1388

Respondent has no specific response.

1389. One former LabMD employee testified that it was understood that when LabMD Billing Department employees played music, the music came from LimeWire or CDs downloaded to their work computers. (CX0714-A ([Fmr. LabMD Empl.], Dep. at 31)).

Response to Finding No. 1389

Respondent has no specific response.

1390. This employee stated that when she would ask Billing Department employees playing music "Where did you get that from?," they told her "It's on LimeWire." (CX0714-A ([Fmr. LabMD Empl.], Dep. at 128-129)).

Response to Finding No. 1390

Respondent objects to this proposed finding of fact because Complaint Counsel misquotes the record. The employee actually testified that "people" would respond "[i]t's on **my** LimeWire." (CX0714-A ([Fmr. LabMD Empl.], Dep. at 128-129)) (emphasis added).

1391. Intentionally left blank.

1392. Intentionally left blank.

7.1.3 1718 File Found on Peer-to-Peer Network

1393. The 1718 File was available on a P2P network, and could be discovered and downloaded by anyone looking for it. (JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 4; Wallace, Tr. 1371-72; CX0730 (Simmons, Dep. at 12, 28-29, 32-34); CX0710-A (Daugherty, LabMD Designee, Dep. at 200-01); CX0738 (Shields Rebuttal Report) ¶¶ 56-58 at 17-18, ¶¶ 65-66 at 19-20); CX0721 (Johnson, Dep. at 104-06)).

Response to Finding No. 1391

Respondent objects to this proposed finding of fact because it is unsupported by the citations to the record. The Joint Stipulations of Fact, Law & Authority stipulate that, "More than 900 files on a computer used by LabMD's billing manager, including the 1718 file were available for sharing through LimeWire." No stipulation was made that "anyone looking for it[]" could discover and download the 1718 File. In addition, the cited testimony of Wallace and Simmons do not support the proposed finding of fact and the cited Daugherty testimony is in direct contrast:

> Q. Is there any reason to believe that the P to P insurance aging file was accessible through the LimeWire, through LimeWire in the billing manager's computer?
>
> A. Is there a reason to believe it was accessible?
>
> Q. Yes.
>
> **A. If someone knew the exact name at the time it was being used, it would have been vulnerable.**

(CX0710 (Daugherty, LabMD Designee, Dep. at 200-201)) (emphasis added).

Finally, with respect to the cited Shields testimony, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). While the cited Johnson testimony does support the proffered finding of fact, the clear weight of the evidence strikes against this portion of Mr. Johnson's testimony.

1394. The 1718 File was found and downloaded using an off-the-shelf peer-to-peer client, such as LimeWire. (Wallace, Tr. 1342-43, 1372, 1440-41). Other LabMD files were downloaded along with the 1718 File. (Wallace, Tr. 1440-41).

Response to Finding No. 1394

Respondent has no specific response.

1395. In May 2008, LabMD was informed that the 1718 File was available on a P2P network, and received a copy that had been downloaded from a P2P network. (Ans. ¶ 17; CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8, Adm. 39; CX0025 (Email J. Boyle to R. Boback Subject: Re: Tiversa/LabMD) at 1; CX0023 (Email J. Boyle to R. Boback Subject: Re: follow-up) at 1; Daugherty, Tr. 981; CX0709 (Daugherty, Dep. at 145-46); CX0710-A (Daugherty, LabMD Designee, Dep. at 32); JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4, Stip. 9).

Response to Finding No. 1395

Respondent has no specific response.

1396. Following LabMD's receipt of the 1718 File, Mr. Boyle acknowledged that he had received and viewed the file. (CX0023 (Email J. Boyle to R. Boback Subject: Re: follow-up) at 1). Mr. Boyle indicated that LabMD had initiated an investigation. (CX0023 (Email J. Boyle to R. Boback Subject: Re: follow-up) at 1).

Response to Finding No. 1396

Respondent has no specific response.

1397. Intentionally left blank.

1398. Intentionally left blank.

7.1.3.1 After Being Notified About Availability of 1718 File, LabMD Discovered LimeWire on a Billing Computer

1399. After being notified in May 2008 that the 1718 File was available through LimeWire, LabMD investigated and determined that LimeWire had been downloaded and installed on a computer used by LabMD's billing department manager (the "Billing Computer") in 2005 or 2006. (Ans. ¶ 18(a); CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) at 4, Resp. to Interrog. 3; CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6; CX0150 (Screenshot: C:\) at 1; CX0730 (Simmons, Dep. at 10); CX0709 (Daugherty, Dep. at 144); CX0736 (Daugherty, IHT at 64-65)).

<u>Response to Finding No. 1399</u>

Respondent has no specific response.

1400. Before being notified in May 2008 that the 1718 File was available on the P2P network, LabMD did not discover that LimeWire was installed on the billing manager's computer. (CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 5-6 (LabMD discovered LimeWire after being contacted regarding 1718 File)).

<u>Response to Finding No. 1400</u>

Respondent has no specific response.

1401. Rosalind Woodson was LabMD's billing department manager in May 2008. (CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6; CX0730 (Simmons, Dep. at 11)).

<u>Response to Finding No. 1401</u>

Respondent has no specific response.

1402. LabMD determined that LimeWire was installed on the Billing Computer when IT employee Alison Simmons inspected LabMD's computers manually to identify which computer(s) were sharing files on P2P network(s). (CX0730 (Simmons, Dep. at 10)).

<u>Response to Finding No. 1402</u>

Respondent has no specific response.

1403. LabMD found that LimeWire was running updates to the P2P application on the Billing Computer as late as April 25, 2008. (CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6).

<u>Response to Finding No. 1403</u>

Respondent has no specific response.

1404. Ms. Simmons took screenshots of the billing manager's computer documenting the existence of LimeWire and the shared 1718 File. (CX0150 (Screenshot: C:\); CX0151 (Screenshot: C:\Program Files\LimeWire); CX0152 (Screenshot: LimeWire: My Shared Files); CX0154 (Screenshot: LimeWire Get Started); CX0155 (Screenshot: Start Menu: LimeWire); CX0156 (Screenshot: LimeWire: Options: Shared Folders); CX0730 (Simmons, Dep. at 14-15, 21, 23-24, 27, 29, 36-37, 42, 112, 150-52)).

Response to Finding No. 1404

Respondent has no specific response.

1405. The version of LimeWire at the time LabMD examined the computer and took screenshots was 4.16.7. (CX0710-A (Daugherty, LabMD Designee, Dep. at 202-03); CX0730 (Simmons, Dep. at 43)).

Response to Finding No. 1405

Respondent has no specific response

1406. After taking screenshots of the billing manager's computer, Ms. Simmons removed LimeWire from the Billing Computer in May 2008. (CX0730 (Simmons, Dep. at 14-15); Ans. ¶ 20).

Response to Finding No. 1406

Respondent has no specific response.

1407. Intentionally left blank.

1408. Intentionally left blank.

7.1.3.2 Hard Drive of Billing Manager's Computer Rendered Inoperable

1409. The hard drive of the computer on which LimeWire was found was removed and was later rendered inoperable in an attempt at a forensic examination. (CX0710-A (Daugherty, LabMD Designee, Dep. at 204-06); Daugherty, Tr. 1088-89).

Response to Finding No. 1409

Respondent has no specific response.

1410. Intentionally left blank.

7.1.4 LabMD Failed to Provide Notice Regarding 1718 File

1411. LabMD did not provide any notice to consumers included in the 1718 File. (CX0710-A (Daugherty, LabMD Designee, Dep. at 48); Daugherty, Tr. 1087).

Response to Finding No. 1411

Respondent has no specific response.

1412. Intentionally left blank.

7.2 Sacramento Incident

7.2.1 Overview

1413. On October 5, 2012, the Sacramento, California Police Department (SPD) found more than 35 LabMD Day Sheets and 9 copied checks and one money order made payable to LabMD in a house in Sacramento, California. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4); CX0087 (*in camera*) (LabMD Day Sheets); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10; CX0720 (Jestes, Dep. at 17-18, 22-23, 33-37).

<u>Response to Finding No. 1413</u>

Respondent has no specific response.

1414. The Sacramento California Police Department found the Day Sheets and checks in the possession of individuals unrelated to LabMD's business who later pleaded no contest to state charges of identity theft. (CX0720 (Jestes, Dep. at 22-23, 44); CX0085 (*in camera*) (LabMD Day Sheets and Copied Checks) at 1-44; CX0087 (*in camera*) (LabMD Day Sheets); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10; CX0107 (Sup. Ct. of Cal.: Erick Garcia Minute Order re Plea) at 1-2; CX0108 (Sup. Ct. of Cal.: Josie Martinez Maldonado Minute Order re Plea) at 1-2).

<u>Response to Finding No. 1414</u>

Respondent has no specific response.

1415. Intentionally left blank.

1416. Intentionally left blank.

7.2.2 October 5, 2012 Investigation

1417. Detective Karina Jestes of the SPD participated in an investigation of 5661 Wilkinson Street initiated on October 5, 2012, along with officer Wilhite, officer Baptista, and officer Morgan. (CX0720 (Jestes, Dep. at 17-18)).

<u>Response to Finding No. 1417</u>

Respondent has no specific response.

1418. The investigation concerned a woman whose utility bill had been compromised and who was then receiving an additional utility bill for an address – 5661 Wilkinson Street in Sacramento – to which she had no connection. (CX0720 (Jestes, Dep. at 17-18)).

<u>Response to Finding No. 1418</u>

Respondent has no specific response.

1419. Intentionally left blank.

1420. Intentionally left blank.

7.2.2.1 Search of 5661 Wilkinson Street

1421. Detective Jestes went to 5661 Wilkinson Street, entered the property, and executed a search. (CX0720 (Jestes, Dep. at 17-19)).

Response to Finding No. 1421

Respondent has no specific response.

1422. No warrant was needed to conduct the search because the occupant of 5661 Wilkinson Street – Erick Garcia – was on searchable probation. (CX0720 (Jestes, Dep. at 18)). According to Detective Jestes, searchable probation means that the police are permitted to enter Mr. Garcia's residence to ensure that he is meeting the terms of his probation. (CX0720 (Jestes, Dep. at 18)).

Response to Finding No. 1422

Respondent has no specific response.

1423. Upon entering the house, Detective Jestes encountered Erick Garcia's wife, Josie Maldonado. (CX0720 (Jestes, Dep. at 18-19)). Ms. Maldonado stated that Mr. Garcia was in a bedroom in the home and pointed to a bedroom. (CX0720 (Jestes, Dep. at 18-19)). Detective Jestes and the other officers located Mr. Garcia, and conducted a search of the house. (CX0720 (Jestes, Dep. at 17-19)).

Response to Finding No. 1423

Respondent has no specific response.

1424. Intentionally left blank.

1425. Intentionally left blank.

7.2.2.2 Items Seized by SPD

1426. The search discovered evidence of utility billing theft, evidence that the occupants of the home were using someone else's name for the gas utility bill, narcotics paraphernalia, narcotics, and several items that Detective Jestes believed showed that identity theft was occurring at the house. (CX0720 (Jestes Dep. at 19-20)).

Response to Finding No. 1426

Respondent has no specific response.

1427. During the search of 5661 Wilkinson Street, the SPD discovered checks that appeared to have been washed, to get rid of the original ink, checks that had preprinted customer information, with new printing added to that information, bills in other people's names for various utilities, and mail. These were all, in Detective Jestes' view, evidence of attempts at identity theft. (CX0720 (Jestes, Dep. at 23-23)).

Response to Finding No. 1427

Respondent has no specific response.

1428. Detective Jestes attempted to contact all of the people whose names were on multiple checks that looked either stolen or washed. She also contacted the original victim of the utility theft, and the new victim of the gas utility theft. (CX0720 (Jestes, Dep. at 26)).

Response to Finding No. 1428

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Detective Jestes' actually testified as follows:

> I attempted to contact all of the **people whose names where [sic] on a lot of the checks that looked like they had been either stolen or washed.** I also tried to – I was not familiar with LabMD; so I tried to figure out basically what LabMD was. I contacted the original victim of the gas utility theft. That's all I can think of right now.

(CX0720 (Jestes, Dep. at 26)). (emphasis added).

1429. When Detective Jestes contacted the individuals whose names were on the checks she learned that most of them had been the victims of some sort of theft, either their mail had been stolen out of the mailbox, or their cars had been broken into. Some had also been victims of identity theft. (CX0720 (Jestes, Dep. at 27)).

Response to Finding No. 1429

Respondent objects to this proposed finding of fact to the extent it suggests that Det. Jestes actually contacted any person whose information appears on the day sheets or the checks associated with the day sheets or that any person whose information appears on the day sheets or the checks associated with the day sheets had been the victim of identity theft. The cited testimony of Detective Jestes does not establish those facts. (CX0720 (Jestes, Dep. at 27)).

1430. The SPD also found more than 35 LabMD Day Sheets and 9 copied checks and one money order made payable to LabMD. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4; CX0720 (Jestes, Dep. at 23); CX0087 (*in camera*) (LabMD Day Sheets) at 1-40; CX0088 (*in camera*) (LabMD Copied Checks) at 1-10).

Response to Finding No. 1430

Respondent has no specific response.

1431. Intentionally left blank.

1432. Intentionally left blank.

7.2.2.2.1 LabMD Documents Found by SPD

7.2.2.2.1.1 Day Sheets

1433. CX0087 contains the Day Sheets found by the SPD during the search of 5661 Wilkinson and later booked into evidence. (CX0720 (Jestes, Dep. at 30-31); CX0087 (*in camera*) (LabMD Day Sheets) at 1-40).

Response to Finding No. 1433

Respondent has no specific response.

1434. The Day Sheets found by the SPD contain Personal Information about at least 600 consumers, including names, Social Security numbers, and in some cases, diagnosis codes. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8, Adm. 38; CX0087 (*in camera*) (LabMD Day Sheets) at 1-40; CX0710-A (Daugherty, LabMD Designee, Dep. at 63, 68-69) (LabMD sent 682 letters to consumers); CX0407 (*in camera*) (Mail Merge List of Persons for LabMD Notification Letter)).

Response to Finding No. 1434

Respondent objects to this proposed finding of fact because it is unsupported by at least one citation to the record. In CX0766, LabMD admitted that "about at least [sic] 500 Consumers, including: names; SSNs; and in some cases, diagnosis codes[]" were included in the "Day Sheets." (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission), at 8 (Admission No. 8).

1435. Some of the Day Sheets found by the Sacramento, California Police Department in October 2012 are dated later than June 5, 2007. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4; CX0087 (*in camera*) (LabMD Day Sheets)).

Response to Finding No. 1435

Respondent has no specific response.

1436. Detective Jestes booked CX0087 into evidence because it appeared to her to be evidence of identity theft. This was because it contained what appeared to be a list of names with Social Security numbers, a billing number, a date, and a monetary amount. She believed this was evidence of identity theft because there was no reason any of the occupants of 5661 Wilkinson should have had such information. Detective Jestes believed that this information could have been used for financial gain or some kind of narcotic gain. (CX0720 (Jestes, Dep. at 33-35)).

Response to Finding No. 1436

Respondent objects to this proposed finding of fact to the extent it suggests that Det. Jestes actually had evidence that the day sheets and the information thereon was used for financial or narcotic gain. The cited testimony of Detective Jestes does not establish those facts. (CX0720 (Jestes, Dep. at 33-35)).

1437. Intentionally left blank.

1438. Intentionally left blank.

7.2.2.2.1.2 Copied Checks

1439. In addition, during the search of 5661 Wilkinson Street, the SPD found 9 copied checks and one money order made payable to LabMD. (CX0720 (Jestes, Dep. at 23, 31-32, 35); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10).

Response to Finding No. 1439

Respondent has no specific response.

1440. CX0088 contains the copies of checks found by the SPD during the search of 5661 Wilkinson and later booked into evidence as Item of Evidence No. 55867-7. (CX0720 (Jestes, Dep. at 31-32); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10).

Response to Finding No. 1440

Respondent has no specific response.

1441. The checks contained consumers' names, addresses, phone numbers, account numbers, and signatures. (CX0720 (Jestes, Dep. at 35); CX0088 (*in camera*) (LabMD Copied Checks) at 1-10).

Response to Finding No. 1441

Respondent has no specific response.

1442. The handwritten notations on pages 4, 7, and 9 of CX0088 were Social Security numbers. (CX0720 (Jestes, Dep. at 35-36)).

Response to Finding No. 1442

Respondent has no specific response.

1443. The handwritten notations on pages 1, 5, and 8 of CX0088 were monetary amounts, and a phone number. (CX0720 (Jestes, Dep. at 36)).

Response to Finding No. 1443

Respondent has no specific response.

1444. Detective Jestes booked CX0088 into evidence because the checks that comprise that exhibit did not have any connection to the house in which they were found, nor to the people who were residing at the house at that time. The people residing in the house should not have possessed account numbers and other personal identifying information. (CX0720 (Jestes, Dep. at 36)).

Response to Finding No. 1444

Respondent objects to this proposed finding of fact because it is an opinion or conclusion, and not a finding of fact.

1445. Intentionally left blank.

1446. Intentionally left blank.

7.2.2.2.1.3 Computers Seized by SPD

1447. Following the October 5, 2012 raid, Detective Jestes returned to the house at 5661 Wilkinson Street, Sacramento, at which time she seized two computers. (CX0720 (Jestes, Dep. at 26)).

Response to Finding No. 1447

Respondent has no specific response.

1448. Detective Jestes believed that the computers might have evidentiary value. (CX0720 (Jestes, Dep. at 37-38)).

Response to Finding No. 1448

Respondent has no specific response.

1449. The seized computers, a desktop and a laptop, were subsequently examined by Detective Shim of the SPD. (CX0720 (Jestes, Dep. at 37-39)).

Response to Finding No. 1449

Respondent has no specific response.

1450. Detective Shim discovered that the desktop computer had been used to access utility billing websites, to search for information regarding use of a child's Social Security number, and to search for the FTC regarding identity theft. He also discovered the presence of peer-to-peer file sharing programs including Vuze and BearShare. (CX0100 (SPD ECU Narrative Report) at 4-5). Based on this report Detective Jestes concluded that this desktop computer was used in perpetrating the utility theft. (CX0720 (Jestes, Dep. at 38-40, 41)).

Response to Finding No. 1450

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Detective Jestes actually testified as follows:

> Q. Based on your training and experience, what conclusions did you draw from the results of Detective Shim's supplementary report and his investigation of the two computers that were seized at 5661 Wilkinson Street?
>
> A. I'm Sorry. Could you repeat that one?
>
> [Record read]
>
> ***A. That specifically the desktop was being used in furtherance of their crimes, specifically regarding the utility billing.***

(CX0720 (Jestes, Dep. at 39) (emphasis added).

1451. On the laptop that was seized from 5661, Wilkinson Street Detective Shim discovered the peer-to-peer filing sharing programs LimeWire and Vuze. (CX0720 (Jestes, Dep. at 40)).

Response to Finding No. 1451

Respondent has no specific response.

1452. Detective Jestes authenticated CX0101 as a true and accurate copy of part of the examination Detective Shim conducted of the desktop computer seized at 5661 Wilkinson Street. (CX0720 (Jestes, Dep. at 41-42)).

Response to Finding No. 1452

Respondent has no specific response.

1453. Intentionally left blank.

1454. Intentionally left blank.

7.2.3 Arrest of Erick Garcia and Josie Maldonado

1455. On October 5, 2012, Erick Garcia was arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. (CX0720 (Jestes, Dep. at 25)).

Response to Finding No. 1455

Respondent has no specific response.

1456. On October 5, 2012, Josie Maldonado was arrested and charged with identity theft, receiving stolen property, possession of methamphetamine, and the possession of narcotics paraphernalia. (CX0720 (Jestes, Dep. at 25)).

Response to Finding No. 1456

Respondent has no specific response.

1457. Mr. Garcia and Ms. Maldonado pled *nolo contendere* to identity theft and were sentenced to probation and a sheriff's work project for the offense identified during the search of 5661 Wilkinson. This is a felony offense even though identity theft can be prosecuted as a misdemeanor. (CX0720 (Jestes, Dep. at 43-45)).

Response to Finding No. 1457

Respondent has no specific response.

1458. Mr. Garcia invoked his Fifth Amendment privilege and refused to testify about how he obtained the Day Sheets and copied checks. (CX0712 (Garcia, Dep. at 24-29)).

Response to Finding No. 1458

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Garcia actually invoked his Fifth Amendment privilege and refused to testify relating to all documents created by LabMD and/or any and all evidence relating to the crime of identity theft. (CX0712 (Garcia, Dep. at 26-27)). The proposed finding of fact mischaracterizes Mr. Garcia's testimony.

1459. Intentionally left blank.

1460. Intentionally left blank.

7.2.4 LabMD Response to Sacramento Incident

7.2.4.1 LabMD Notice to Affected Consumers

1461. LabMD sent 682 letters to the consumers included in the Sacramento documents on March 27 or 28, 2013. (CX0710-A (Daugherty, LabMD Designee, Dep. at 63, 68-69); CX0709 (Daugherty, Dep. at 120); CX0227 (LabMD Letter to Consumers re: Sacramento Incident, unaddressed) at 1-2).

Response to Finding No. 1461

Respondent has no specific response.

1462. LabMD sent notices to consumers by comparing the numbers located on the Day Sheets with other information in its possession. (CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) at 4, Resp. to Interrog. 6).

Response to Finding No. 1462

Respondent has no specific response.

1463. LabMD retrieved contact information for consumers in the Day Sheets by entering the billing number into Lytec. (CX0710-A (Daugherty, LabMD Designee, Dep. at 61-62)).

Response to Finding No. 1463

Respondent has no specific response.

1464. CX0407 is the list of consumers LabMD created for sending out the notification letters. (CX0710-A (Daugherty, LabMD Designee, Dep. at 64-65); CX0407 (*in camera*) (Mail Merge List of Persons for LabMD Notification Letter) at 1-13).

Response to Finding No. 1464

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. LabMD's designee, Michael Daugherty testified as follows:

> Q. During discovery in this case LabMD's counsel has represented that document CX 407 is responsive to a request for production 16 which asks for, quote, all documents relating to communication with consumers regarding any security incident, to put it in context.
>
> A. (Witness examining document). Okay.

> Q. Is this the list of consumers that Trisha Gilbreth ***created identifying the names and addresses of consumers who were included in the documents found by the Sacramento Police Department?***
>
> A. I'm not sure if it's exactly Trisha that created it.
>
> Q. Is this, is this a list of consumers that LabMD created?
>
> A. Yes, I believe so.
>
> Q. On this list only the names are included -- let me backtrack and ask you--
>
> A. No, it's more than that.
>
> Q. Let me ask you a different question.

(CX0710-A (Daugherty (LabMD Designee), Dep. at 64-65) (emphasis added).

1465. The letter provided an Atlanta-area phone number that went to voicemail, which was monitored by LabMD employees. (CX0710-A (Daugherty, LabMD Designee, Dep. at 76)).

<u>Response to Finding No. 1465</u>

Respondent has no specific response.

1466. The number was active through December 2013. (CX0710-A (Daugherty, LabMD Designee, Dep. at 76)).

<u>Response to Finding No. 1466</u>

Respondent has no specific response.

1467. LabMD does not know how many people called the number in response to the letter. (CX0710-A (Daugherty, LabMD Designee, Dep. at 78)).

Response to Finding No. 1467

Respondent objects to this proposed finding of fact to the extent it ignores testimony in the record establishing how many people responded to the notification (76) and how many people actual took the insurance (50% of those responding) (CX0710-A (Daugherty, LabMD Designee, Dep. at 78)), in order to establish the fact that LabMD did not know how many people responded using the hotline number.

1468. LabMD did not hire a call center. (CX0710-A (Daugherty, LabMD Designee, Dep. at 76)).

Response to Finding No. 1468

Respondent has no specific response.

1469. LabMD provided an email address, monitored by its attorney Stephen Fusco, in the notification letter. (CX0710-A (Daugherty, LabMD Designee, Dep. at 80); CX0227 (LabMD Notification Letter to Consumers – Unaddressed) at 1-2).

Response to Finding No. 1469

Respondent has no specific response.

1470. Intentionally left blank.

1471. Intentionally left blank.

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.

8.1 LabMD's Unreasonable Security Practices Caused or are Likely to Cause Substantial Injury to Consumers

8.1.1 Identity Theft

8.1.1.1 The Definition of Identity Theft

1472. Identity theft occurs when someone uses another person's identity without his or her permission. (Kam, Tr. 394; CX0742 (Kam Report) at 10).

Response to Finding No. 1472

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1473. Identity theft can include using another person's name, address, date of birth, Social Security number, credit card and banking information, drivers license, or any combination of these types of personal identifiers to impersonate another person. (Kam, Tr. 394; CX0742 (Kam Report) at 10).

Response to Finding No. 1473

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1474. Identity fraud is the unauthorized use of some portion of another person's information to achieve illicit financial gain. (Kam, Tr. 395; CX0742 (Kam Report) at 10; CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1474

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1475. "Identity theft" is also sometimes referred to as "identity fraud." (Van Dyke, Tr. 577; CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1475

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1476. A person's name, address, date of birth, Social Security number (SSN), credit card and banking information, and drivers' license is collectively known as personally identifiable information (PII). (CX0742 (Kam Report) at 10). PII, as used by Mr. Kam, is a subset of the data in Personal Information. (CX0742 (Kam Report) at 10; *supra* ¶ 12 (definition of Personal Information)).

Response to Finding No. 1476

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1477. Intentionally left blank.

1478. Intentionally left blank.

8.1.1.2 Identity Fraud Categories

1479. Identity fraud subtypes include new account fraud (NAF), existing non-card fraud (ENCF), and existing card fraud (ECF). (Van Dyke, Tr. 591; CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1479

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1480. Existing card fraud (ECF) is identity fraud perpetrated through the use of existing credit or debit cards and/or their account numbers. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1480

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1481. Existing non-card fraud (ENCF) is identity fraud perpetrated through the use of existing checking or savings accounts or existing loans, insurance, telephone and utilities accounts, along with income tax fraud and medical identity fraud. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1481

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1482. New account fraud (NAF) is a form of identity fraud perpetrated through the use of another person's personally identifiable information to open new fraudulent accounts. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1482

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1483. Medical identity theft occurs when someone uses another person's medical identity to fraudulently receive medical services, prescription drugs and goods, as well as attempts to fraudulently bill private and public health insurance entities. (Kam, Tr. 395-96; CX0742 (Kam Report) at 11).

Response to Finding No. 1483

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1484. Medical identity fraud is the unauthorized use of a third party's personally identifiable information to obtain medical products or services, including but not limited to office visits and consultations, medical operations, and prescriptions. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1484

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1485. Intentionally left blank.

1486. Intentionally left blank.

8.1.1.3 How Identity Theft is Committed

1487. Identity thieves can use PII to commit numerous crimes, such as creating fake credentials like drivers' licenses and birth certificates; opening new accounts for credit cards, retail store cards and mail-order accounts; taking over legitimate victim accounts resulting in fraudulent purchases; opening new bank accounts; check counterfeiting and forgery; filing fraudulent tax returns; payday loan fraud; and employment fraud. (Kam, Tr. 382-85, 394-95; CX0742 (Kam Report) at 10-11).

Response to Finding No. 1487

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1488. The type of information compromised directly corresponds to the types of fraud that can be committed with the information. (CX0741 (Van Dyke Report) at 5).

Response to Finding No. 1488

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact to the extent it suggests that the 1718 file was compromised. In his expert report, Van Dyke defined unauthorized disclosure of the 1718 file as being found at "four IP addresses." (CX0741 (Van Dyke Report) at 8.). The 1718 file was not found at any of the four IP addresses contained in CX0019. (Wallace, Tr. 1383). Thus, any of Van Dyke's analysis regarding exposure of information in the 1718 file is irrelevant.

1489. In combination with a consumer's name, Social Security numbers can be used to gain direct access to financial accounts, including credit card, checking, and savings accounts, which are frauds falling under Existing Non-Card Fraud (ENCF) and Existing Card Fraud (ECF). (CX0741 (Van Dyke Report) at 5; *see also* Van Dyke, Tr. 613).

Response to Finding No. 1489

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1490. Social Security numbers can be combined with a consumer's name, address, and phone number (legitimate or not) to establish a new fraudulent account, which is a New Account Fraud (NAF). (CX0741 (Van Dyke Report) at 5).

Response to Finding No. 1490

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1491. Credit or debit card information can be used to make an unauthorized purchase without the presence of the legitimate credit or debit card, which is an Existing Card Fraud (ECF). (CX0741 (Van Dyke Report) at 5).

Response to Finding No. 1491

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1492. The following types of information are valuable to identity thieves: Social Security numbers, birth dates, driver's license numbers, bank account numbers, credit card numbers, personal identification numbers, passwords, and health insurance policy numbers. (CX0720 (Jestes, Dep. at 14-15)).

Response to Finding No. 1492

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1493. Identity theft, identity fraud and medical identity theft cause a wide range of economic and non-economic harms to consumers. (CX0742 (Kam Report) at 23).

Response to Finding No. 1493

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1494. Intentionally left blank.

1495. Intentionally left blank.

8.1.1.4 Notifications Inform Consumers of Unauthorized Disclosures and Resulting Risk of Harm From Identity Theft

1496. Data breach notification laws require organizations that have been breached to give notice to consumers that a breach occurred. (Kam, Tr. 400; CX0742 (Kam Report) at 17).

Response to Finding No. 1496

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1497. Notification laws have been enacted by states to alert affected consumers of a breach so they can take actions to reduce their risk of harm from identity crime. (Kam, Tr. 400; CX0742 (Kam Report) at 17).

Response to Finding No. 1497

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1498. Without a notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information. (Kam, Tr. 401, 417; CX0742 (Kam Report) at 17).

Response to Finding No. 1498

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1499. Without knowing about the unauthorized disclosures, consumers are put at a risk of possible harms from identity crimes, including medical identity theft. (CX0742 (Kam Report) at 8).

Response to Finding No. 1499

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1500. Intentionally left blank.

1501. Intentionally left blank.

8.1.1.4.1 Notifications Do Not Remediate All Consumer Harms

1502. Even if consumers receive notice of the unauthorized disclosure of their PII, consumers cannot avoid all harms from identity theft. (CX0742 (Kam Report) at 17).

Response to Finding No. 1502

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1503. Studies show that consumers who are notified that their information has been disclosed in a breach are at an elevated risk of falling victim to various identity crimes. (Kam, Tr. 400-01, 463; CX0742 (Kam Report) at 17).

Response to Finding No. 1503

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1504. Intentionally left blank.

1505. Intentionally left blank.

8.1.1.5 The Rate of Identity Theft is Higher Among Consumers Who Have Been a Victim of a Breach

1506. Consumers whose PII was compromised in a data breach are significantly more likely to suffer identity fraud than those consumer who did not have their PII compromised in a data breach. (CX0741 (Van Dyke Report) at 6).

Response to Finding No. 1506

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1507. Nearly one in three data breach victims (30.5%) also fell victim to identity fraud in 2013. (Kam, Tr. 483; CX0742 (Kam Report) at 11; Van Dyke, Tr. 624-25; CX0741 (Van Dyke Report) at 6).

Response to Finding No. 1507

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1508. Only 2.7% of all Americans who were not notified that their information was compromised in a data breach in the last 12 months reported becoming a victim of identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 6).

Response to Finding No. 1508

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1509. The difference between the rate of fraud of data breach victims and non-data breach victims is a ten-to-one general increased likelihood that a data breach will lead to actual fraud victimization. (CX0741 (Van Dyke Report) at 6).

Response to Finding No. 1509

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1510. Of consumers who had their SSN compromised in an unauthorized disclosure in 2013, 7.1% suffer NAF within twelve months of being notified their SSN was disclosed. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1510

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1511. Of consumers who had their SSN compromised in an unauthorized disclosure in 2013, 7.1% suffer ENCF within twelve months of being notified their SSN was disclosed. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1511

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1512. Of consumers who had their SSN compromised in an unauthorized disclosure in 2013, 13.1% suffer ECF within twelve months of being notified their SSN was disclosed. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1512

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1513. Intentionally left blank
.

1514. Intentionally left blank.

8.1.1.5.1 Consumer Harm from Identity Theft for Consumers Whose Information was Disclosed in an Unauthorized Disclosure

1515. Consumers affected by an unauthorized disclosure of their PII will experiences significant harm as a result of suffering a variety of fraud types, including ECF, ENCF, and NAF. (CX0741 (Van Dyke Report) at 8).

Response to Finding No. 1515

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1516. Intentionally left blank.

8.1.1.5.1.1 Impact of New Account Fraud (NAF) on Consumers

8.1.1.5.1.1.1 Financial Harm

1517. Consumers who are victims of NAF incur, on average, $449 in consumer costs (or out-of-pocket costs incurred by the victim) to resolve a fraud case. (Van Dyke, Tr. 593; CX0741 (Van Dyke Report) at 9).

Response to Finding No. 1517

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1518. Consumers who are victims of NAF fall prey to crimes that total over $2,968 ("fraud amount") on average. (CX0741 (Van Dyke Report) at 9).

Response to Finding No. 1518

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1519. Intentionally left blank.

1520. Intentionally left blank.

8.1.1.5.1.1.2 Time Loss

1521. NAF victims spend, on average, 26 hours of their own time resolving the fraud. (Van Dyke, Tr. 595; CX0741 (Van Dyke Report) at 9).

Response to Finding No. 1521

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1522. NAF is the most time-consuming fraud to resolve because the accounts have been established at an institution with which the victim did not previously have an established relationship. Without a pre-existing relationship, the institution must solicit significantly more information from the victim to positively establish that he or she is legitimate and not responsible for opening the fraudulent account. (CX0741 (Van Dyke Report) at 9-10).

Response to Finding No. 1522

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1523. Documentation required to close an account in the case of NAF could include a filed police report, along with a notarized assertion of fraud. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1523

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1524. The victim may have to spend more time resolving NAF fraud when there is a need for removal of fraudulent accounts from a consumer credit bureau report(s). (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1524

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1525. Consumers included in the Sacramento Day Sheets are at risk of NAF. (*Infra* § 9.4.2.2 (Likely NAF Impact on Consumers From Unauthorized Disclosures of the Sacramento Day Sheets) (¶¶ 1742-1746)).

Response to Finding No. 1525

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1526. Intentionally left blank.

1527. Intentionally left blank.

8.1.1.5.1.2 Impact of Existing Non-Card Fraud (ENCF) on Consumers

8.1.1.5.1.2.1 Financial Harm

1528. Consumers who are victims of ENCF, on average, incur $207 in consumer costs. (Van Dyke, Tr. 593; CX0741 (Van Dyke Report) at 9).

Response to Finding No. 1528

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1529. Victims of ENCF fall prey to crimes that total over $1,805 on average. (CX0741 (Van Dyke Report) at 97).

Response to Finding No. 1529

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1530. Intentionally left blank.

1531. Intentionally left blank.

8.1.1.5.1.2.2 Time Loss

1532. Consumers who are ENCF victims spend, on average, 16 hours of their own time resolving the fraud. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1532

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1533. ENCF fraud can involve various account types, many of which do not offer substantial protections for consumer from liability for unauthorized transactions. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1533

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1534. The process for resolving fraud with accounts that do not offer substantial protections for consumer from liability for unauthorized transactions could require a victim to provide a notarized assertion of fraud and other documentation. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1534

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1535. A victim of ENCF may need to obtain legal counsel if the victim's assertion of fraud is challenged. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1535

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1536. Consumers included in the Sacramento Day Sheets are at risk of ENCF. (*Infra* § 9.4.2.3 (Likely ENCF Impact on Consumers From the Unauthorized Disclosure of the Sacramento Day Sheets) (¶¶ 1749-1753).

<u>Response to Finding No. 1536</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1537. Intentionally left blank.

1538. Intentionally left blank.

8.1.1.5.1.3 Impact of Existing Card Fraud (ECF) on Consumers

8.1.1.5.1.3.1 Financial Harm

1539. Consumers who are victims of ECF on average incur $106 in consumer costs. (Van Dyke, Tr. 593; CX0741 (Van Dyke Report) at 9).

<u>Response to Finding No. 1539</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1540. Consumers who are victims of ECF fall prey to crimes that total over $1,373 on average. (CX0741 (Van Dyke Report) at 9).

Response to Finding No. 1540

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1541. Consumers included in the Sacramento Day Sheets are at risk of ECF. (*Infra* § 9.4.2.4 (Likely ECF Impact on Consumers From the Unauthorized Disclosure of the Sacramento Day Sheets) (¶¶ 1756-1760)).

Response to Finding No. 1541

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1542. Intentionally left blank.

1543. Intentionally left blank.

8.1.1.5.1.3.2 Time Loss

1544. ECF victims spend, on average, 9 hours of their own time resolving the fraud. (Van Dyke, Tr. 595-96; CX0741 (Van Dyke Report) at 10).

<u>Response to Finding No. 1544</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1545. Intentionally left blank.

8.1.1.5.2 Victims May Have Difficulty Mitigating Loss

8.1.1.5.2.1 Difficulty Closing Fraudulent Accounts

1546. Consumer costs (also known as out-of-pocket costs) incurred by the victim to resolve a fraud case may include: postage, copying, notarizing of documents, lost wages from time taken off of work, legal fees, and payment of fraudulent debts to avoid further problems. (Van Dyke, Tr. 591-92; CX0741 (Van Dyke Report) at 9).

<u>Response to Finding No. 1546</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1547. A victim of identity theft may have to clean up multiple fraudulent accounts. (Kam, Tr. 394-95; CX0742 (Kam Report) at 13).

<u>Response to Finding No. 1547</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1548. Consumers who are victims need to contact each of the entities with which a fraudulent account was opened to dispute the charges and close the accounts. (Kam, Tr. 419; CX0742 (Kam Report) at 13).

Response to Finding No. 1548

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1549. In many cases, the closure of the fraudulent accounts requires following up, submitting copies of a police report, identity theft affidavit, proof of residence, and identification. (CX0742 (Kam Report) at 13).

Response to Finding No. 1549

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1550. In many cases, the victim may have to follow up several times to ensure his or her accounts are corrected and all negative records created by the identity thieves are expunged. (CX0742 (Kam Report) at 13).

Response to Finding No. 1550

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1551. Documentation required to close an account in the case of NAF could include a filed police report, along with a notarized assertion of fraud. (CX0741 (Van Dyke Report) at 10).

Response to Finding No. 1551

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1552. Intentionally left blank.

1553. Intentionally left blank.

8.1.1.5.3 Victims May Be Falsely Arrested on Criminal Charges

1554. If criminal acts are committed under a stolen identity, the victim may only know of it when he or she is arrested. (CX0742 (Kam Report) at 14).

Response to Finding No. 1554

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1555. If criminal acts are committed under a stolen identity, the identity thief's arrest may be part of a background check on the victim. (CX0742 (Kam Report) at 14).

Response to Finding No. 1555

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1556. The identity thief's arrest being part of the background check can affect security clearances, drivers' licenses, and other career opportunities. (CX0742 (Kam Report) at 14).

Response to Finding No. 1556

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1557. Intentionally left blank.

1558. Intentionally left blank.

8.1.1.5.4 Victims May Experience Tax Identity Theft

1559. Consumers who are victims of identity theft can be affected by identity thieves submitting fraudulent tax returns. (Kam, Tr. 384; CX0742 (Kam Report) at 14).

Response to Finding No. 1559

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1560. Tax identity theft can prevent consumers who are victims of tax identity theft from being able to file their tax returns and obtain refunds. (Kam, Tr. 384; CX0742 (Kam Report) at 14).

Response to Finding No. 1560

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1561. The delay in receiving the refund can extend to be as long as six months. (CX0742 (Kam Report) at 14).

Response to Finding No. 1561

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1562. The delay in receiving the refund materially impacts consumer victims' cash flow. (CX0742 (Kam Report) at 14).

Response to Finding No. 1562

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1563. Intentionally left blank.

1564. Intentionally left blank.

8.1.1.5.5 Consumers May be Vulnerable to Identity Theft Harms For a Long Period of Time

1565. Some PII cannot be readily replaced by consumers, such as names, addresses, and Social Security numbers (SSNs). (CX0741 (Van Dyke Report) at 5).

Response to Finding No. 1565

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1566. The types of PII that rarely change can be used fraudulently for extended periods of time once compromised, placing consumers at risk of injury indefinitely. (Kam, Tr. 412-14; CX0742 (Kam Report) at 22; Van Dyke, Tr. 460; CX0741 (Van Dyke Report) at 5).

Response to Finding No. 1566

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1567. A number of identity theft victims continue to be harmed, as identity thieves resell the victims' sensitive Personal Information to other identity thieves, perpetuating the harms for years. (Kam, Tr. 412-14; CX0742 (Kam Report) at 12).

Response to Finding No. 1567

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1568. Intentionally left blank.

1569. Intentionally left blank.

8.1.1.5.5.1 SSNs are Especially Valuable Pieces of Information to Identity Thieves for a Long Period of Time

1570. The unauthorized disclosure of SSNs creates an opportunity for identity theft and identity frauds to be committed against consumers over a long period of time. (Kam, Tr. 412, 414, 473, 479; CX0742 (Kam Report) at 22).

Response to Finding No. 1570

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1571. Identity theft and identity frauds can happen over a long period of time because consumers do not typically change their SSNs after being notified of a breach. (Kam, Tr. 412-13, 473, 479; CX0742 (Kam Report) at 22).

Response to Finding No. 1571

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1572. Changing an SSN can be a cumbersome process and does not necessarily solve all problems a consumer may experience as a result of an unauthorized disclosure of his or her SSN. (Kam, Tr. 443-44; CX0742 (Kam Report) at 22).

<u>Response to Finding No. 1572</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1573. A new SSN will not necessarily solve a victim's problems because government agencies and private businesses maintain records under consumers' old SSNs. (Kam, Tr. 443-44; CX0742 (Kam Report) at 22).

<u>Response to Finding No. 1573</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1574. A new SSN will not necessarily solve a victim's problems because credit reporting agencies may use the victim's old SSN to identify credit records. (CX0742 (Kam Report) at 22).

<u>Response to Finding No. 1574</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1575. Because consumers rarely change their SSNs, these numbers can be fraudulently used for extended periods of time, placing consumers at heightened risk of injury. (CX0741 (Van Dyke) at 5).

<u>Response to Finding No. 1575</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1576. Intentionally left blank.

1577. Intentionally left blank.

8.1.1.6 Process for Remediation of Identity Theft Harms

8.1.1.6.1 Identity Theft Harms Can Take Months to Years to Identify

1578. It may take months or years for a consumer to learn that his or her sensitive Personal Information was disclosed without authorization. (Kam, Tr. 465-66; CX0742 (Kam Report) at 12).

<u>Response to Finding No. 1578</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1579. It may take months or years for a consumer to learn that his or her sensitive Personal Information was misused to commit an identity crime. (CX0742 (Kam Report) at 12).

Response to Finding No. 1579

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1580. It may take months or years for a consumer to learn his or her information was misused to commit an identity crime because identity criminals commit a wide variety of identity fraud, some of which may be difficult for the consumer to detect. (CX0742 (Kam Report) at 12).

Response to Finding No. 1580

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1581. Intentionally left blank.

1582. Intentionally left blank.

8.1.1.6.2 Identity Theft Harms are Difficult to Remediate Once Identified

1583. Some consumers who are victims of identity theft must deal with several identity fraud issues. (Kam, Tr. 395-96; CX0742 (Kam Report) at 12).

Response to Finding No. 1583

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1584. Once a consumer's information is exposed, it is difficult for that consumer to detect and prevent additional misuse of his or her information; the consumer has no control over who accesses this information since identity thieves will resell their information to other identity thieves, perpetuating the harms for years. (Kam, Tr. 396; CX0742 (Kam Report) at 8, 12).

Response to Finding No. 1584

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1585. Intentionally left blank.

1586. Intentionally left blank.

8.1.1.6.3 Identity Fraud is Increasing

1587. In 2010, nearly 1 in 9 Americans notified of a data breach suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

Response to Finding No. 1587

Respondent objects to this proposed finding of fact as the timeframe to which the proposed finding of fact is unclear. In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1588. In 2011, 1 in 5 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

Response to Finding No. 1588

Respondent objects to this proposed finding of fact as the timeframe to which the proposed finding of fact is unclear. In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1589. In 2012, 1 in 4 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

Response to Finding No. 1589

Respondent objects to this proposed finding of fact as the timeframe to which the proposed finding of fact is unclear. In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the

ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1590. In 2013, 1 in 3 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

Response to Finding No. 1590

Respondent objects to this proposed finding of fact as the timeframe to which the proposed finding of fact is unclear. In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1591. Intentionally left blank.

1592. Intentionally left blank.

8.1.2 Medical Identity Theft

1593. A person’s medical identity is comprised of a number of personal data elements, such as name, medical record number, health insurance number, other demographics, charge amounts for services, Social Security number, Medicare number (which contain a person’s nine-digit SSN), date of birth, financial account information, patient diagnosis (such as International Classification of Diseases (ICD) and Current Procedural Terminology Codes (CPT)). (Kam, Tr. 396, 411; CX0742 (Kam Report) at 11-12).

Response to Finding No. 1593

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1594. This type of information is included in the 1718 File and the Day Sheets. (*Infra* §§ 9.3.1 (The 1718 File Contains Sensitive Consumer Information) (¶¶ 1661-1664), 9.4.1 (The Sacramento Day Sheets and Checks Had Sensitive Information) (¶¶ 1714-1719)).

Response to Finding No. 1594

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1595. Health insurance policy information and SSNs can be used to commit medical identity frauds. CX0741 (Van Dyke Report) at 13).

Response to Finding No. 1595

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1596. Medical identity theft is a serious problem. (CX0742 (Kam Report) at 12).

Response to Finding No. 1596

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1597. Medical identity theft affects an estimated 1.84 million Americans. (CX0742 (Kam Report) at 12).

Response to Finding No. 1597

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1598. Intentionally left blank.

1599. Intentionally left blank.

8.1.2.1 Consumers Experience Financial Harm Due to Medical Identity Theft

1600. The costs consumers who are victims of medical identity theft incur include reimbursement to healthcare providers for services received by the identity thief; money spent on identity protection, credit counseling, and legal counsel; and payment for medical services and prescriptions because of a lapse in healthcare coverage. (Kam, Tr. 421, 422; CX0742 (Kam Report) at 15).

Response to Finding No. 1600

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1601. Medical identity frauds can burden consumers with financial costs related to unpaid medical bills from unauthorized procedures, products, or services. (CX0741 (Van Dyke Report) at 13).

Response to Finding No. 1601

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1602. Thirty-six percent of medical identity theft victims incurred an average of $18,660 in out-of-pocket expenses. (Kam, Tr. 422; CX0742 (Kam Report) at 19).

Response to Finding No. 1602

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Kam's Report, CX0742, actually states that 36% of victims of medical identify theft, of **one 2013 survey**, paid **an average** of $18,660 in out of pocket costs. (CX0742 (Kam Report) at 19) (emphasis added). Complaint Counsel's attempt to extrapolate this survey to, presumably, all "medical identity theft victims" should not be permitted by this court.

In addition, Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1603. The $18,660 figure comprises: (1) reimbursement to healthcare providers for unauthorized services or procedures; (2) funds spent on identity protection, credit counseling, and legal counsel; and (3) payment for medical services and prescriptions because of a lapse in healthcare coverage. (CX0742 (Kam Report) at 15).

Response to Finding No. 1603

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1604. Intentionally left blank.

1605. Intentionally left blank.

8.1.2.2 Consumers Experience Reputational Harm Due to Medical Identity Theft

1606. Reputational harm can occur from the loss of sensitive personal health information. (Kam, Tr. 395-96, 412, 421; CX0742 (Kam Report) at 16).

Response to Finding No. 1606

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1607. Consumers can suffer when information disclosing that they have a stigmatized condition is disclosed. (Kam, Tr. 447-48; CX0742 (Kam Report) at 16).

Response to Finding No. 1607

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1608. Consumers who are medical identity theft victims and have sexually transmitted diseases are particularly sensitive to having their condition disclosed. (Kam, Tr. 447-48; CX0742 (Kam Report) at 16).

Response to Finding No. 1608

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1609. Consumers who are medical identity theft victims and who have cancer may be sensitive to having their condition disclosed. (Kam, Tr. 447-48; CX0742 (Kam Report) at 16).

Response to Finding No. 1609

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1610. Intentionally left blank.

1611. Intentionally left blank.

8.1.2.3 Other Harms Consumers Experience Due to Medical Identity Theft

8.1.2.3.1 Integrity of Consumer Health Records Compromised Due to Medical Identity Theft Causes a Risk of Physical Harm to Consumers

1612. Consumers who are victims of medical identity theft may have the integrity of their electronic health record compromised if the health information of the identity thief has merged with that of the victim. (Kam, Tr. 426-27; CX0742 (Kam Report) at 15).

Response to Finding No. 1612

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1613. When a consumer's electronic health record is compromised and the health information of the identity thief merges with that of the consumer, the resulting inaccuracies could pose a serious risk to the health and safety of the medical identity theft victim by, for instance, associating the wrong blood type with the victim or obscuring life-threatening drug allergy information. (Kam, Tr. 426-27, 428-30; CX0742 (Kam Report) at 15).

Response to Finding No. 1613

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1614. Consumers who are victims of medical identity theft may suffer from misdiagnosis of illness, delay in receiving medical treatment, mistreatment of illness, or wrong pharmaceuticals prescribed. (Kam, Tr. 426-30; CX0742 (Kam Report) at 16).

Response to Finding No. 1614

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1615. As a result of medical identity theft, an illness could be misdiagnosed, causing serious health implications, including the potential death of the consumer. (Kam, Tr. 428, 464; CX0742 (Kam Report) at 16).

Response to Finding No. 1615

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1616. One study has found that 15% of medical identity victims had a misdiagnosis of illness, 14% had a delay in receiving medical treatment, 13% had a mistreatment of illness, and 11% had wrong pharmaceuticals prescribed. (CX0742 (Kam Report) at 16).

Response to Finding No. 1616

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1617. Direct physical harm to the consumer could occur, for example, when a change is made to consumer's medical record that could result in improper or unnecessary treatments. (CX0741 (Van Dyke Report) at 13).

Response to Finding No. 1617

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1618. Medical identity fraud has the potential to be a lifelong threat to both the peace-of-mind and physical well-being of consumers whose PII was compromised. (CX0741 (Van Dyke Report) at 14).

Response to Finding No. 1618

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1619. Intentionally left blank.

1620. Intentionally left blank.

8.1.2.3.2 Consumers May Experience a Loss of Healthcare Due to Medical Identity Theft

1621. A survey in 2013 found that thirty-nine percent of medical identity theft victims lost their healthcare coverage. (CX0742 (Kam Report) at 15).

Response to Finding No. 1621

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1622. Intentionally left blank.

8.1.2.3.3 The Process for Remediating Medical Identity Theft is Difficult

8.1.2.3.3.1 Consumers May Experience Time Loss Attempting to Resolve Medical Identity Theft

1623. Consumers spend a significant amount of time resolving the problems caused by medical identity theft. (Kam, Tr. 441-42; CX0742 (Kam Report) at 15).

Response to Finding No. 1623

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1624. The amount of time required to solve the crime can discourage consumers who are victims of medical identity theft from even trying to fix the problem of medical identity theft. (Kam, Tr. 441-43; CX0742 (Kam Report) at 15).

Response to Finding No. 1624

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1625. Intentionally left blank.

1626. Intentionally left blank.

8.1.2.3.3.2 The Lack of a Central Regulating Bureau for Medical Identity Theft Makes Remediation Difficult for Consumers Who Are Victims

1627. Unlike credit bureaus, which are required by law to accept consumer fraud alerts, there is no central medical identity bureau where a consumer can set up a fraud alert. (Kam, Tr. 420-21, 510; CX0742 (Kam Report) at 14; 15 U.S.C. 1681c-1).

Response to Finding No. 1627

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1628. The consumer has no way of notifying healthcare providers or payers of the potential fraud, or to receive consumer alerts. (Kam, Tr. 510; CX0742 (Kam Report) at 14).

Response to Finding No. 1628

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1629. A result of the consumer’s inability to notify healthcare providers or payers of the potential fraud is that identity thieves can use a consumer’s medical identity to commit identity crimes. (Kam, Tr. 510; CX0742 (Kam Report) at 14).

<u>Response to Finding No. 1629</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1630. Many hospitals and clinics do not have staff training or internal processes to help victims of identity theft and medical identity theft. (CX0742 (Kam Report) at 14).

<u>Response to Finding No. 1630</u>

1631. Intentionally left blank.

1632. Intentionally left blank.

8.1.3 Medical Identity Fraud

1633. Medical identity fraud can burden consumers with financial costs related to unpaid medical bills from unauthorized procedures, products, or services. (CX0741 (Van Dyke Report) at 13).

<u>Response to Finding No. 1633</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1634. Medical identity fraud can burden consumers with direct physical harm in those cases where a change is made to a consumer’s medical records that could result in improper or unnecessary treatments. (CX0741 (Van Dyke Report) at 13).

<u>Response to Finding No. 1634</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1635. In 2012, 355,425 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 13, 14).

Response to Finding No. 1635

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1636. In 2011, 449,462 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

Response to Finding No. 1636

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1637. In 2010, 426,026 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

Response to Finding No. 1637

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1638. In 2009, 824,581 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

Response to Finding No. 1638

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1639. In 2008, 567,484 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

Response to Finding No. 1639

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1640. Intentionally left blank

1641. Intentionally left blank.

8.2 LabMD's Security Failures Placed All Consumers Whose Personal Information is on Their Network at Risk.

8.2.1 LabMD Stores the Types of Information Used to Commit Identity Frauds

1642. LabMD maintains Personal Information on its computer network for more than 750,000 consumers, including: first and last name; telephone number; address; date of birth; SSN; medical record number; bank routing, account, and check numbers; credit or debit card information; laboratory test result, medical test code, or diagnosis, or clinical history; and health insurance company name and policy number. (*Supra* § 4.6.1 (Amount of Personal Information Collected) *et seq.* (¶¶ 78-161).

Response to Finding No. 1642

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1643. The types of information LabMD maintains on its computer networks are the types of information needed to perpetrate frauds. (CX0741 (Van Dyke Report) at 6, 12).

Response to Finding No. 1643

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1644. Intentionally left blank.

1645. Intentionally left blank.

8.2.1.1 Healthcare Organizations are Targets for Cyber Criminals Because of the Repositories of Sensitive Data They Possess

1646. Healthcare organizations possess high value sensitive medical information. (Kam, Tr. 413, 558; CX0742 (Kam Report) at 23).

Response to Finding No. 1646

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The portions of the record cited to not contain testimony or expert opinion to support the proposition that Healthcare organizations possess high value sensitive medical information.

1647. Cyber criminals are targeting healthcare organizations because of the high value of sensitive medical information. (Kam, Tr. 519; CX0742 (Kam Report) at 23).

Response to Finding No. 1647

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1648. Organizations with inadequate data security programs are vulnerable to unauthorized disclosures of sensitive Personal Information. (CX0742 (Kam Report) at 23).

Response to Finding No. 1648

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1649. Because healthcare systems are the target of cyber thieves, there is an increased risk of data theft and fraud for healthcare systems. (CX0742 (Kam Report) at 23).

Response to Finding No. 1649

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1650. The consumer PII maintained by LabMD is a target of data thieves. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1650

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

In addition, Respondent objects because the proposed finding of fact mischaracterizes Mr. Van Dyke's expert report and attempts to prospectively apply the retroactive conclusions contained in his report. The cited portions of the report state:

> Consumers' [PII] is a target of data thieves. This would include all of the personally identifiable information maintained by LabMD regarding consumers, including: first and last name; address; date of birth; telephone number; Social Security number; medical record number; bank routing, account, and check numbers; credit or debit card information; laboratory test result, medical test code, or diagnosis, or clinical history; health insurance company name and policy number. It is my opinion that

> all of this information is valuable in the commission of fraud. While LabMD is known to have disclosed without authorization the information in the "Insurance Aging Report" and "Day Sheets", LabMD's failure to provide reasonable and appropriate security for the PII it maintains on its computer networks risked exposing 750,000 consumers to a likelihood of a wide variety of frauds, including NAF, ENCF, ECF and medical identity fraud.

(CX0741 (Van Dyke Report) at 12).

Here, even if Mr. Van Dyke's Report was of sound basis, which it is not, it applies retroactively to LabMD's alleged past practices. Complaint Counsel's attempt to apply this report prospectively should not be permitted.

1651. Intentionally left blank.

1652. Intentionally left blank.

8.2.2 LabMD's Failure to Secure the Personal Information it Stores Places Consumers at Greater Risk of Identity Theft

1653. LabMD's failure to use reasonable measures to prevent unauthorized access to sensitive Personal Information creates an elevated risk of unauthorized disclosure of this information. (CX0742 (Kam Report) at 10, 23).

Response to Finding No. 1653

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Kam was asked to "assume[ ] that LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0742 (Kam Report) at 5).

1654. This elevated risk is likely to cause substantial harm to consumers in the form of identity theft, medical identity theft, and other harms. (CX0742 (Kam Report) at 23).

Response to Finding No. 1654

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1655. LabMD's failure to employ reasonable measures to prevent unauthorized access to consumers' Personal Information is likely to cause substantial harm, including harm stemming from medical identity theft. (CX0742 (Kam Report) at 8).

Response to Finding No. 1655

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Kam was asked to "assume[ ] that LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0742 (Kam Report) at 5).

1656. There is a risk of harm to consumers when a company fails to protect sensitive Personal Information. (CX0742 (Kam Report) at 10).

Response to Finding No. 1656

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1657. LabMD's failure to provide reasonable security for this information places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of identity theft. (CX0741 (Van Dyke Report) at 3).

Response to Finding No. 1657

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Van Dyke was asked to "assume[ ] that LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0741 (Van Dyke Report) at 2).

1658. LabMD's failure to provide reasonable security for the PII it maintains on its computer networks risks exposing 750,000 consumers to a likelihood of a wide variety of identity frauds, including NAF, ENCF, ECF, and medical identity fraud. (CX0741 (Van Dyke Report) at 12-13).

Response to Finding No. 1658

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Van Dyke was asked to "assume[ ] that LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0741 (Van Dyke Report) at 2). In addition, Respondent objects because the proposed finding of fact mischaracterizes Mr. Van Dyke's expert report and attempts to prospectively apply the retroactive conclusions contained in his report. The cited portions of the report state:

> …LabMD's failure to provide reasonable and appropriate security for the PII it maintains on its computer networks ***risked exposing*** 750,000 consumers to a likelihood of a wide variety of identify frauds, including NAF, ENCF, ECF and medical identity fraud.

(CX0741 (Van Dyke Report) at 12-13) (emphasis added).

Here, even if Mr. Van Dyke's Report was of sound basis, which it is not, it applies retroactively to LabMD's alleged past practices. Complaint Counsel's attempt to apply this report prospectively should not be permitted.

1659. Intentionally left blank.

1660. Intentionally left blank.

8.3 Substantial Consumer Injury from Unauthorized Disclosure of the 1718 File

8.3.1 The 1718 File Contains Sensitive Consumer Information

1661. The 1718 File includes consumer first and last names; middle initials; dates of birth; nine-digit Social Security numbers; health insurance provider numbers, names, addresses, and phone numbers; Current Procedural Terminology (CPT) diagnostic codes; billing dates and amounts. (Kam, Tr. 411; CX0742 (Kam Report) at 18; CX0741 (Van Dyke Report) at 2; CX0008-0011 (*in camera*), CX0697 (*in camera*) (1718 File)).

Response to Finding No. 1661

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1662. The 1718 File contains the information of approximately 9,300 consumers. (Ans. ¶ 19); CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 8, Adm. 37); CX0008-0011 (*in camera*), CX0697 (*in camera*) (1718 File)).

Response to Finding No. 1662

Respondent has no specific response.

1663. The 1718 File was available to individuals not authorized to have the information. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4; Ans. ¶ 17)).

Response to Finding No. 1663

Respondent has no specific response.

1664. An unauthorized disclosure of the 1718 File was made in May 2008. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4).

Response to Finding No. 1664

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Complaint Counsel, at best, misstates the evidence contained in JX0001. There is no stipulation contained in the Joint Stipulations of Law, Fact and Authenticity that support this proposed finding of fact. In fact in May 2008, LabMD was told that Tiversa had found the 1718 File on a peer-to-peer network. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4 ¶ 9).

1665. Intentionally left blank.

1666. Intentionally left blank.

8.3.2 Identity Thieves Frequently Use the Types of Information in the 1718 File to Commit Identity Theft

1667. Identity thieves frequently use the types of information in the 1718 File – including names, dates of birth, nine-digit Social Security numbers, and health insurance and billing information – to commit identity crimes. (Kam, Tr. 396, 411 CX0742 (Kam Report) at 10, 18); CX0741 (Van Dyke Report) at 6, 12).

Response to Finding No. 1667

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1668. Consumers whose sensitive Personal Information was exposed in the 1718 File are at a significantly higher risk than the general public of becoming a victim of identity theft and medical identity theft, or of experiencing other privacy harms. (CX0742 (Kam Report) at 19).

Response to Finding No. 1668

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1669. Consumers whose sensitive Personal Information was exposed in the 1718 File are at significant risk of harm from identity crimes due to the unauthorized disclosure of their sensitive Personal Information. (Kam, Tr. 410; CX0742 (Kam Report) at 9).

Response to Finding No. 1669

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1670. LabMD's failure to provide reasonable security for information – including names, dates of birth, Social Security number, and health insurance and billing information – places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of identity theft. (CX0741 (Van Dyke Report) at 3).

<u>Response to Finding No. 1670</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Van Dyke was asked to "assume[ ] that LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0741 (Van Dyke Report) at 2).

1671. The disclosure of names with corresponding Social Security numbers, health insurance provider numbers, and CPT diagnostic codes pose a greater risk of various identity crimes. (Kam, Tr. 471, CX0742 (Kam Report) at 18).

<u>Response to Finding No. 1671</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1672. Intentionally left blank.

1673. Intentionally left blank.

8.3.3 Identity Theft Likely Caused By Disclosure of 1718 File

1674. LabMD's failures that resulted in the 1718 File being available to individuals not authorized to have the information caused or is likely to cause substantial injury to consumers in the form of identity theft, including medical identity theft. See *supra* §§ 9.3.1 (The 1718 File Contains Sensitive Consumer Information) (¶¶ 1661-1664), 9.3.2 (Identity Thieves Frequently Use the Types of Information in the 1718 File to Commit Identity Theft) (¶¶ 1667-1671); *infra* § 9.3.4 (Impact on Consumers From Medical Identity Theft Stemming From Unauthorized Disclosure of the 1718 File) *et seq.* (¶¶ 1678-1711)).

<u>Response to Finding No. 1674</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1675. LabMD's failure to provide reasonable security for the information in the 1718 File places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of identity theft. (CX0741 (Van Dyke Report) at 2-3).

<u>Response to Finding No. 1675</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact because it is predicated on an assumption. Van Dyke was asked to "assume[ ] that

LabMD failed to provide reasonable and appropriate security for consumer's personal information maintained on its computer networks." (CX0741 (Van Dyke Report) at 2).

1676. Intentionally left blank.

1677. Intentionally left blank.

8.3.4 Impact on Consumers From Medical Identity Theft Stemming From Unauthorized Disclosure of the 1718 File

1678. The availability of the 1718 File to unauthorized individuals that resulted from LabMD's failures caused or is likely to cause substantial injury to consumers in the form of medical identity theft. (*Infra* § 9.3.4.1 (Consumers Will Suffer Reputational and Other Harms Stemming from Unauthorized Disclosure of the 1718 File) *et seq.* (¶¶ 1684-1701)).

<u>Response to Finding No. 1678</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.)

1679. Identity thieves frequently use the types of information compromised – including names, dates of birth, nine-digit Social Security numbers, and health insurance and billing information – to commit identity crimes. (Kam, Tr. 396, 410-11; CX0742 (Kam Report) at 10, 18); CX0741 (Van Dyke Report) at 6, 12).

<u>Response to Finding No. 1679</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1680. When a consumer falls victim to medical identity theft, that consumer could experience financial harms as well as a host of non-financial harms, including physical harm from misdiagnoses or unnecessary treatments. (Kam Tr. 464; CX0742 (Kam Report) at 15-16).

Response to Finding No. 1680

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1681. Medical identity theft can damage a consumer's economic well-being and reputation, and even risk his or her health. CX0742 (Kam Report) at 8).

Response to Finding No. 1681

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1682. Intentionally left blank.

1683. Intentionally left blank.

8.3.4.1 Consumers Will Suffer Reputational and Other Harms Stemming from Unauthorized Disclosure of the 1718 File

8.3.4.1.1 Unauthorized Disclosure of CPT Codes Revealing Sensitive Conditions is Likely to Cause Harm

1684. CPT codes are sensitive information that was disclosed by LabMD in the 1718 File. (Kam, Tr. 445-47; CX0742 (Kam Report) at 21); *infra* ¶¶ 1685-1692).

Response to Finding No. 1684

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

Respondent objects to this proposed finding of fact to the extent Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that infra or supra should also not be used.

1685. Several of the CPT codes in the 1718 File indicate tests for sensitive conditions. (Kam, Tr. 447-49; CX0742 (Kam Report) at 21).

Response to Finding No. 1685

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1686. Among the sensitive conditions are CPT codes that indicate tests for the presence of prostate cancer, testosterone levels, or sexually transmitted diseases, specifically HIV, hepatitis, and herpes. (Kam, Tr. 447-49; CX0742 (Kam Report) at 21).

Response to Finding No. 1686

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1687. Disclosure of the performance of these tests could cause embarrassment or other negative outcomes, including reputational harm and changes to life, health, or disability insurance, to these consumers. (CX0742 (Kam Report) at 21).

Response to Finding No. 1687

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1688. There were 3,195 instances of the CPT code 84153; 548 instances of the CPT code 84154; and 109 instances of CPT code G0103. (Kam, Tr. 449-50; CX0742 (Kam Report) at 21). These CPT codes relate to tests for prostate specific antigens, which are an indication of possible prostate cancer. (Kam, Tr. 450; CX0742 (Kam Report) at 21). More than 3,000 consumers had these CPT codes linked to their name. (Kam, Tr. 450; CX0742 (Kam Report) at 21).

Response to Finding No. 1688

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1689. There were 134 instances of CPT code 84402 and 435 instances of CPT code 84403. (CX0742 (Kam Report) at 21). These CPT codes relate to tests for testosterone levels. (CX0742 (Kam Report) at 21). Testosterone levels can be used to evaluate men for testicular dysfunction. (CX0742 (Kam Report) at 21). Low levels of testosterone in men may cause reduced fertility or lack of libido. (CX0742 (Kam Report) at 21). More than 400 consumers had these CPT codes linked to their name. (Kam, Tr. 450; CX0742 (Kam Report) at 21).

Response to Finding No. 1689

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1690. Nineteen consumers had one or more of the following CPT codes 86694; 86695; and 86696, which are CPT codes that indicate tests for herpes. (Kam, Tr. 450-51; CX0742 (Kam Report) at 21).

Response to Finding No. 1690

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and

analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1691. Six consumers had one or more of these CPT codes: 86705 and 86706, which are CPT codes relate to Hepatitis B or Hepatitis C. (Kam, Tr. 451; CX0742 (Kam Report) at 21).

Response to Finding No. 1691

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1692. There were 13 instances of CPT code 86689, which is a CPT code that indicates a test for HIV. (Kam, Tr. 451; CX0742 (Kam Report) at 21).

Response to Finding No. 1692

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1693. Intentionally left blank.

1694. Intentionally left blank.

8.3.4.1.2 There is a Significant Risk of Consumer Reputational Harm Due to the Unauthorized Disclosure of the CPT Codes

1695. There is a significant risk of reputational damage for 3,000 or more consumers from the unauthorized disclosure of sensitive medical information. (CX0742 (Kam Report) at 9).

Response to Finding No. 1695

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1696. The significant risk of reputational harm is specifically for the consumers whose diagnostic codes indicate tests for prostate cancer, herpes, hepatitis, HIV, and testosterone levels. (Kam, Tr. 447-48, CX0742 (Kam Report) at 9).

Response to Finding No. 1696

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1697. Disclosure of the fact that tests were performed could cause embarrassment or other negative outcomes, including reputational harm and changes to insurance for these consumers, including life, health, and disability insurance. (Kam, Tr. 411-12; CX0742 (Kam Report) at 21).

Response to Finding No. 1697

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1698. Intentionally left blank.

1699. Intentionally left blank.

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

1700. Once health information is disclosed, it is impossible to restore a consumer's privacy. (Kam, Tr. 414, 453; CX0742 (Kam Report) at 8, 21).

<u>Response to Finding No. 1700</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1701. Once a consumer's sensitive personal data is disclosed without authorization, that consumer has no control over who accesses this information. CX0742 (Kam Report) at 8.

<u>Response to Finding No. 1701</u>

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1702. Intentionally left blank.

1703. Intentionally left blank.

8.3.4.2 Consumers Did Not Receive Notice of the Unauthorized Disclosure of the 1718 File.

1704. LabMD did not notify the 9,300 consumers whose Personal Information was contained in the 1718 File. (CX0710-A (Daugherty Designee Dep.) at 48).

<u>Response to Finding No. 1704</u>

Respondent has no specific response.

1705. Consumers who do not get notified of a disclosure of their Personal Information are at risk of possible harms from identity crimes, including medical identity theft. (*Supra* § 9.1.1.4 (Notifications Inform Consumers of Unauthorized Disclosures and Resulting Risk of Harm From Identity Theft) (¶¶ 1496-1499)).

<u>Response to Finding No. 1705</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1706. Intentionally left blank.

1707. Intentionally left blank.

8.3.4.3 With No Notification of Unauthorized Disclosure, No Mitigation of Harm is Possible

1708. The 9,300 consumers in the 1718 File have had no opportunity to mitigate the risk of harm because LabMD has not notified the consumers of the unauthorized disclosure. (Kam, Tr. 418-19; CX0742 (Kam Report) at 9, 19).

Response to Finding No. 1708

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1709. Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information. (Kam, Tr. 400-01; CX0742 (Kam Report) at 17).

Response to Finding No. 1709

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1710. Notifications are intended to alert affected consumers of a breach so that they can take actions to reduce their risk of harm from identity crime. (Kam, Tr. 419; CX0742 (Kam Report) at 17); *see also* Kam, Tr. 417-19, CX0742 (Kam Report) at 9, 19 (consumers included in the 1718 File had no opportunity to reduce risk of falling victim to identity crimes due to LabMD's failure to notify them).

Response to Finding No. 1710

Respondent objects because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1711. However, once consumers' Personal Information has been used in identity theft or identity fraud, including medical identity theft or fraud, complete remediation is not possible. (*Infra* § 9.4.2.5.1 (Consumers Cannot Avoid All Harms Through Notification of Unauthorized Disclosures of Information) (¶¶ 1769-1770)).

Response to Finding No. 1711

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1712. Intentionally left blank.

1713. Intentionally left blank.

8.4 Substantial Consumer Injury From Unauthorized Disclosure of the Sacramento Day Sheets and Checks

8.4.1 The Sacramento Day Sheets and Checks Had Sensitive Information

1714. The compromised data contained on the nine checks found in the Sacramento incident included: first and last names; middle initials; address; nine-digit Social Security number; bank routing and account numbers; amounts; signatures' handwritten comments that appear to be SSNs, check numbers and amounts. (CX0085 (*in camera*) (LabMD Day Sheets and Copied Checks); CX0088 (*in camera*) LabMD Copied Checks); CX0720 (Jestes, Dep. at 35); Kam, Tr. 454-55; CX0742 (Kam Report) at 21-22).

<u>Response to Finding No. 1714</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited portions of the record do not provide support for the proposed finding of fact that the data in question was "compromised."

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1715. The "Chart" column on LabMD's Day Sheets is the patient identification number, which can be a Social Security number or a date of birth. (CX0733 (Boyle, IHT at 52-53)).

<u>Response to Finding No. 1715</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Boyle's testimony actually states as follows:

> Q. Okay. What is entered in the chart? There's – there's a series of columns here. The first one is CHART. What do you enter in the CHART column?
>
> A. The – that would be the patient identify – identification number.

> Q. And what would that be?
>
> A. It could be a couple of things. It could be the social security number.
>
> Q. Yeah.
>
> A. It could be the medical record number with an account abbreviation associated to it. And it could be an – it could be a date of birth with initials combination followed by an account abbreviation.

(CX0733 (Boyle, IHT at 52-53)).

1716. The "Name" column on LabMD's Day Sheets is the patient's name. (CX0733 (Boyle, IHT at 53)).

Response to Finding No. 1716

Respondent has no specific response.

1717. The compromised data in the Sacramento Day Sheets included first and last names; middle initial; nine-digit Social Security numbers; billing dates, and amounts. (CX0087 (*in camera*) (LabMD Day Sheets); CX0085 (*in camera*) (LabMD Day Sheets and Copied Checks); CX0720 (Jestes, Dep. at 32-35); Kam, Tr. 454-455; CX0742 (Kam Report) at 21-22)).

Response to Finding No. 1717

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. The cited portions of the record do not provide support for the proposed finding of fact that the data in question was "compromised."

1718. The Day Sheets and Checks found by the Sacramento Police Department were in the possession of individuals who pleaded no contest to state charges of identity theft contain consumers' names and SSNs. (CX0720 (Jestes, Dep. at 35-37, 43-44); CX0107 (Plea of Erick Garcia); CX0108 (Plea of Josie Maldonado); CX0741 (Van Dyke Report) at 2).

Response to Finding No. 1718

Respondent has no specific response.

1719. The unauthorized disclosure of this information could be used to commit identity fraud. (Kam, Tr. 458-59; CX0742 (Kam Report) at 22; CX0741 (Van Dyke Report) at 6).

<u>Response to Finding No. 1719</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1720. Intentionally left blank.

1721. Intentionally left blank.

8.4.2 Harms Stemming From the Unauthorized Disclosure of the Sacramento Day Sheets and Checks

1722. The forty pages of Day Sheets and the nine checks were found in the possession of two individuals on October 5, 2012, who pleaded "no contest" to identity theft. (CX0720 (Jestes, Dep. at 36-37, 43-44); CX0107 (Plea of Erick Garcia); CX0108 (Plea of Josie Maldonado)).

<u>Response to Finding No. 1722</u>

Respondent has no specific response.

1723. Approximately 600 consumers were affected by the Sacramento disclosure. (CX0085 (*in camera*) (LabMD Day Sheets and Copied Checks); CX0087 (*in camera*) (LabMD Day Sheets); CX0088 (*in camera*) (LabMD Copied Checks)).

<u>Response to Finding No. 1723</u>

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Simply put, the proposed finding of fact is a legal conclusion.

In addition, Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.,* 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses). Respondent further objects to this proposed finding of fact to the extent it suggests that consumers were injured as a result of the day sheets being found in Sacramento. There is no evidence in the record that any "consumers were affected by the Sacramento disclosure."

1724. There were approximately 600 SSNs of LabMD consumers in the Sacramento Day Sheets. (CX0087 (*in camera*) (LabMD Day Sheets); CX0451 (*in camera*) (Sacrementoresults7.xlsx Native File)[1]).

Response to Finding No. 1724

Respondent has no specific response.

1725. There is the likelihood of substantial risk of injury to the 600 consumers from the exposure of the Sacramento Day Sheets and copied checks. (Kam, Tr. 458-59).

Response to Finding No. 1725

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II*, *Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1726. The approximately 600 consumers whose Personal Information was contained in the LabMD documents found in Sacramento are at risk of harm from identity crimes. (CX0742 (Kam Report) at 10).

Response to Finding No. 1726

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II*, *Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

[1] Complaint Counsel made an offer of proof of CX0451 to the Court on May 21, 2014. (Tr. 371-73). Complaint Counsel is preserving its exception to the Court's ruling denying admission of the document, and includes this reference to reserve its right to appeal the exclusion of the document.

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1727. The fact that known identity thieves acquired this information increases the possibility that the crime of identity theft occurred. (CX0742 (Kam Report) at 22; CX0741 (Van Dyke Report) at 8).

<u>Response to Finding No. 1727</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1728. The fact that known identity thieves acquired this information increases the possibility that the crime of identity theft occurred is based on who had access to and viewed the data. (CX0742 (Kam Report) at 22).

<u>Response to Finding No. 1728</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1729. The fact that the Day Sheets and copied checks were found with other evidence of identity theft speaks to the value of the consumer information in the documents and the likelihood that it may have been misused. (CX0720 (Jestes, Dep. at 22-23, 27, 34-35); CX0742 (Kam Report) at 22-23).

<u>Response to Finding No. 1729</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250,

at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1730. LabMD's failure to provide reasonable security for sensitive Personal Information is likely to cause substantial injury to consumers. (CX0742 (Kam Report) at 9).

Response to Finding No. 1730

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1731. LabMD's failure to provide reasonable security for sensitive Personal Information puts consumers at a significant risk of identity crimes. (CX0742 (Kam Report) at 9).

Response to Finding No. 1731

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1732. Given that the consumer data was found in the hands of known identity thieves, these estimates of harm should be viewed as a floor versus universe of potential harms that could befall the consumers involved. (Kam, Tr. 560; CX0742 (Kam Report) at 17).

Response to Finding No. 1732

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1733. LabMD's failure to provide reasonable security for this information places consumers, whose information LabMD maintains, at significantly higher risk of becoming a victim of identity theft. (CX0741 (Van Dyke Report) at 2-3).

Response to Finding No. 1733

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1734. Intentionally left blank.

1735. Intentionally left blank.

8.4.2.1 Likely Harm to Consumers From Unauthorized Disclosure of the Sacramento Day Sheets

1736. There are 164 anticipated cases of fraud (NAF, ENCF, and ECF) due to the unauthorized disclosure of the Sacramento Day Sheets. (Van Dyke, Tr. 619; CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1736

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1737. The anticipated fraud amount due to frauds (NAF, ENCF, and ECF) stemming from the unauthorized disclosure of the Sacramento Day Sheets is $311,248. (Van Dyke, Tr. 623; CX0741 (Van Dyke Report) at 12).

<u>Response to Finding No. 1737</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1738. The anticipated consumer cost due to frauds (NAF, ENCF, and ECF) stemming from the unauthorized disclosure of the Sacramento Day Sheets is $36,277. (Van Dyke, Tr. 620; CX0741 (Van Dyke Report) at 12).

<u>Response to Finding No. 1738</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1739. The anticipated number of hours required to resolve frauds (NAF, ENCF, and ECF) stemming from the unauthorized disclosure of the Sacramento Day Sheets is 2,497 hours. (Van Dyke, Tr. 622; CX0741 (Van Dyke Report) at 12).

<u>Response to Finding No. 1739</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1740. Intentionally left blank.

1741. Intentionally left blank.

8.4.2.2 Likely NAF Impact on Consumers From Unauthorized Disclosure of the Sacramento Day Sheets

1742. The incidence rate of NAF fraud for victims who were notified that their SSN was disclosed without authorization in a data breach in the last 12 months was 7.1%. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1742

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1743. There are 43 anticipated cases of NAF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1743

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1744. The anticipated fraud amount due to NAF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $126,437. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1744

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1745. The anticipated consumer cost due to NAF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $19,127. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1745

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1746. The anticipated number of hours required to resolve NAF stemming from the unauthorized disclosure of the Sacramento Day Sheets is 1,108 hours. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1746

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1747. Intentionally left blank.

1748. Intentionally left blank.

8.4.2.3 Likely ENCF Impact on Consumers From Unauthorized Disclosure of the Sacramento Day Sheets

1749. The incidence rate of ENCF fraud for victims who were notified that their SSN was disclosed without authorization in a data breach in the last 12 months was 7.1%. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1749

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1750. There are 43 anticipated cases of ENCF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1750

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1751. The anticipated fraud amount due to ENCF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $76,893. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1751

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1752. The anticipated consumer cost due to ENCF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $8,818. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1752

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1753. The anticipated number of hours required to resolve ENCF stemming from the unauthorized disclosure of the Sacramento Day Sheets is 682 hours. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1753

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1754. Intentionally left blank.

1755. Intentionally left blank.

8.4.2.4 Likely ECF Impact on Consumers From the Unauthorized Disclosure of the Sacramento Day Sheets

1756. The incidence rate of ECF fraud for victims who were notified that their SSN was disclosed without authorization in a data breach in the last 12 months was 13.1%. (CX0741 (Van Dyke Report) at 11).

Response to Finding No. 1756

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1757. There are 79 anticipated cases of ECF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1757

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1758. The anticipated fraud amount due to ECF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $107,918. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1758

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1759. The anticipated consumer cost due to ECF stemming from the unauthorized disclosure of the Sacramento Day Sheets is $8,332. (CX0741 (Van Dyke Report) at 12).

Response to Finding No. 1759

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that

summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1760. The anticipated number of hours required to resolve ECF stemming from the unauthorized disclosure of the Sacramento Day Sheets is 707 hours. (CX0741 (Van Dyke Report) at 12).

<u>Response to Finding No. 1760</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1761. Intentionally left blank.

1762. Intentionally left blank.

8.4.2.5 LabMD's Notification to the Sacramento Consumers Does Not Eliminate All Risk of Harm to Those Consumers

1763. Even though LabMD provided notice to the consumers in the Sacramento Day Sheets and Checks, there is a strong possibility some of the consumers will still fall victim to identity theft and identity fraud. (Kam, Tr. 400-01; CX0742 (Kam Report) at 22).

<u>Response to Finding No. 1763</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1764. Notification does not eliminate the risk of harm from identity crime to consumers. (Kam, Tr. 420; CX0742 (Kam Report) at 17).

<u>Response to Finding No. 1764</u>

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1765. Approximately 12% of the consumers notified of the LabMD Day Sheets and Checks found in Sacramento sought credit monitoring. (CX0742 (Kam Report) at 23, CX0710-A (Daugherty, LabMD Designee, Dep. at 84-85; CX0407 (*in camera*) (Mail Merge List of Persons for LabMD Notification Letter) at 40-43).

<u>Response to Finding No. 1765</u>

Respondent has no specific response.

1766. Credit monitoring does not alleviate all harms consumers may experience as a result of an unauthorized disclosure of their Personal Information. See *supra* §§ 9.1.1.5.1.1.2 (Time Loss) (¶¶ 1521-1525), 9.1.1.5.1.2.2 (Time Loss) (¶¶ 1532-1536), 9.1.1.5.1.3.2 (Time Loss) (¶ 1544), 9.1.1.5.3 (Victims May Be Falsely Arrested on Criminal Charges), 9.1.1.5.4 (Victims May Experience Tax Identity Theft) (¶¶ 1554-1556)).

<u>Response to Finding No. 1766</u>

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

1767. Intentionally left blank.

1768. Intentionally left blank.

8.4.2.5.1 Consumers Cannot Avoid All Harms Through Notification of Unauthorized Disclosures of Information

1769. Breach notification does not eliminate the risk of harm from identity crime to consumers. (Kam, Tr. 420; CX0742 (Kam Report) at 17).

Response to Finding No. 1769

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II*, *Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1770. Even if LabMD has provided notice to consumers, consumers would still remain at risk of harm from identity crimes since this unauthorized disclosure included Social Security numbers and health insurance numbers, which can be used to commit identity crimes over an extended period of time. (Kam, Tr. 412-14, 420; CX0742 (Kam Report) at 9).

Response to Finding No. 1770s

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1771. Intentionally left blank.

1772. Intentionally left blank.

8.5 The Harm Caused or Likely to Be Caused by LabMD's Practices is Not Reasonably Avoidable by the Consumers Themselves

8.5.1 The Consumer Is Not in a Position to Know of a Company's Security Practices

1773. A consumer cannot know about the security practices of every company that collects or maintains his or her Personal Information. (Kam, Tr. 398; CX0742 (Kam Report) at 17).

Response to Finding No. 1773

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1774. Consumers have no way of knowing independently about an organization's unauthorized disclosure of their sensitive Personal Information. (Kam, Tr. 401; CX0742 (Kam Report) at 17). 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. (Kam, Tr. 398-401).

Response to Finding No. 1774

Respondent objects to this proposed finding of fact because it is an expert opinion or conclusion, and not a finding of fact. *See In re Realcomp II, Ltd.*, 2009 FTC LEXIS 250, at *9 n.4 (2009) (commission opinion adopting findings of fact by the ALJ that summarized the opinions expressed and analysis conducted by an expert witness without any implication that they endorsed such opinions or analyses).

1775. Intentionally left blank.

1776. Intentionally left blank.

8.5.1.1 Consumers Were Not in a Position to Know of LabMD's Security Practices

8.5.1.1.1 Consumers Did Not Know LabMD Would Test Their Specimen and Receive Their Personal Information

1777. Consumers needing medical tests would not know LabMD would test their specimen. (*Infra* ¶¶ 1778-1782).

Response to Finding No. 1777

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

1778. SUN did not inform consumers that their specimens were going to be tested by LabMD. (CX0726 (Maxey, SUN Designee, Dep. at 78)).

Response to Finding No. 1778

Respondent has no specific response.

1779. Consumers would not know that their specimen given to SUN was being tested by LabMD unless their insurance provider made a request for a specific lab and the patient knew the insurance plan's specific request. (CX0726 (Maxey, SUN Designee, Dep. at 78)).

Response to Finding No. 1779

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Maxey actually testified as follows:

> Q. So a patient would not know which lab was testing their specimen?
>
> A. That's correct, ***except if they knew that if their insurance – a specific request was for Aetna***. But if someone had another insurance plan that was not lab specific, they wouldn't know.

(CX0726 (Maxey, SUN Designee, Dep. at 78)) (emphasis added).

1780. Consumers who had their specimen processed at SUN would not know that LabMD had their Personal Information. (CX0726 (Maxey, SUN Designee, Dep. at 80-81, 100-101)).

Response to Finding No. 1780

Respondent has no specific response.

1781. Midtown did not inform consumers that their specimens were going to be sent to LabMD unless the patient inquired. (CX0728 (Randolph, Midtown Designee, Dep. at 67)).

Response to Finding No. 1781

Respondent has no specific response.

1782. The great majority of consumers did not know the specimen they gave to Midtown was going to LabMD. (CX0728 (Randolph, Midtown Designee, Dep. at 67)).

Response to Finding No. 1782

Respondent has no specific response.

1783. Intentionally left blank.

1784. Intentionally left blank.

8.5.1.1.2 Consumers Have No Way of Knowing LabMD's Data Security Practices, Even If They Knew LabMD was Getting Their Personal Information

1785. Consumers have no knowledge of LabMD's data security practices before their specimen is sent. (*Infra* ¶¶ 1786-1787).

Response to Finding No. 1785

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

1786. Consumers could not have known what LabMD's security practices were before the patient's specimen was sent to LabMD. (CX0726 (Maxey, SUN Designee, Dep. at 79)).

Response to Finding No. 1786

Respondent has no specific response.

1787. Consumers who gave a specimen to Midtown that was then processed by LabMD would not know what LabMD's data security practices were. (CX0728 (Randolph, Midtown Designee, Dep. at 67)).

Response to Finding No. 1787

Respondent has no specific response.

1788. Intentionally left blank.

1789. Intentionally left blank.

8.5.1.2 The Physician Clients Were Not Routinely Informed About LabMD's Data Security Practices

1790. LabMD's physician clients were not informed about LabMD's data management practices unless they expressed concern. (CX0718 (Hudson, Dep. at 52-54)). Only a few physician clients expressed concern about LabMD's management of their data. (CX0718 (Hudson, Dep. at 52-54)).

Response to Finding No. 1790

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Hudson's testimony is devoid of any basis for the proposed finding of fact that "LabMD's physician clients were not informed about LabMD's data management practices unless they expressed concern." Respondent has no specific response to the remainder of the proposed finding of fact.

1791. If physician clients asked sales representatives about whether the collection of all of their patients' information was HIPAA compliant, sales representatives would inform them that LabMD gathered their entire practice's patient data to "simplify and expedite your lab requisition and lab results process." (CX0718 (Hudson, Dep. at 67)).

Response to Finding No. 1791

Respondent objects to this proposed finding of fact because it is unsupported by the citation to the record. Mr. Hudson testified about how he, hypothetically, would have responded to physician clients. Complaint Counsel's attempt to expand this testimony beyond the hypothetical testimony as it related to Mr. Hudson provided should not be permitted.

1792. Intentionally left blank.

1793. Intentionally left blank.

8.5.1.2.1 Sales Representatives Assured Physician Clients that Data at LabMD Was Secure

1794. Sales representatives assured physician clients that their data was on secure servers. (CX0718 (Hudson, Dep. at 67-68)).

Response to Finding No. 1794

Respondent has no specific response.

1795. Sales representatives' assurances about security were based on what they were told in their sales and management training. (CX0718 (Hudson, Dep. at 68)).

Response to Finding No. 1795

Respondent objects to this proposed finding of fact to the extent it suggests that Hudson did not personally believe that the data was secure and only made this statement as a result of being told to do so in training.

1796. Intentionally left blank.

1797. Intentionally left blank.

8.6 The Harm Caused or Likely to Be Caused by LabMD's Practices is Not Outweighed by Countervailing Benefits to Consumers or Competition

1798. LabMD could have corrected its unreasonable security failings at low or no cost, and its failure to do so provided no benefit to consumers or competition. (*Supra* § 6 (LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low Cost Measures) *et seq.* (¶¶ 1113-1185)).

Response to Finding No. 1798

Respondent objects to this proposed finding of fact because Complaint Counsel fails to cite to specific references to the evidentiary record, but instead cites to other paragraphs in these findings of fact. *See* Order on Post-Trial Briefs, *In the Matter of LabMD, Inc.*, FTC Dkt. No. 9357, at 2 (July 16, 2015) (mandating that "[a]ll proposed findings of fact shall be supported by specific references to the evidentiary record"); *see also* at 3 (stating "[d]o not use '*Id.*' as a cite for proposed findings of fact . . .," implying that *infra* or *supra* should also not be used.).

1799. Intentionally left blank.

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

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

DATED: SEPTEMBER 3, 2015

COUNSEL FOR RESPONDENT

CERTIFICATE OF SERVICE

I hereby certify that on September 3, 2015, I caused to be filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system, which will send an electronic notification of such filing to the Office of the Secretary:

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

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

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

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

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

Dated: September 3, 2015 /s/ Patrick J. Massari

CERTIFICATE OF ELECTRONIC FILING

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

Dated: September 3, 2015 /s/ Patrick J. Massari

Notice of Electronic Service

I hereby certify that on September 03, 2015, I filed an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply to Complaint Counsel's Proposed Findings of Fact, with:

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

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

I hereby certify that on September 03, 2015, I served via E-Service an electronic copy of the foregoing Respondent LabMD, Inc.'s Reply to Complaint Counsel's Proposed Findings of Fact, upon:

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

Hallee Morgan
Cause of Action
cmccoyhunter@ftc.gov
Respondent

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

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

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

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

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

Alain Sheer
Federal Trade Commission
asheer@ftc.gov
Complaint

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

Megan Cox
Federal Trade Commission
mcox1@ftc.gov
Complaint

Ryan Mehm
Federal Trade Commission
rmehm@ftc.gov
Complaint

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

Patrick Massari
Attorney