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

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
08 10 2015
578646
SECRETARY
ORIGINAL

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

COMPLAINT COUNSEL'S PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

Alain Sheer
Laura Riposo VanDruff
Ryan Mehm
Megan Cox
Jarad Brown

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

Complaint Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Regulations

Cases

<u>Other Authorities</u>

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.

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.

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.

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.

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

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.

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.

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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

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

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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[1]; 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).

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).

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

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

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)).

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

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

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

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

[1] Complaint Counsel has not marked as nonpublic its proposed findings of fact and conclusions of law that cite to *in camera* exhibits CX0008-CX0011, CX0697, CX0085, CX0087, CX0088, CX0407, CX0451, and RX645 where (1) the exhibit has been granted *in camera* status due to the inclusion of Sensitive Personal Information as defined in Rule 3.45(b) and (2) the citation is to the existence or nature of the exhibit, or to general information about the exhibit as a whole, rather than to specific Sensitive Personal Information contained therein.

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)).

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)).

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)).

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).

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).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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).

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).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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

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).

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).

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)).

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)).

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).

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)).

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)).

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)).

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).

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

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)).

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)).

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)).

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)).

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

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)).

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. (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).

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).

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)).

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)).

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)).

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).

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

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

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)).

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).

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).

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

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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

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

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)).

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

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)).

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)).

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)).

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)).

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

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)).

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

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)).

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)).

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)).

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)).

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)).

162. Intentionally left blank.

3.7 LabMD's Computer Network

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

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)).

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)).

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).

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

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).

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).

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).

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)).

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)).

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).

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

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)).

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)).

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

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)).

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

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

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)).

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)).

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)).

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)).

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

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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

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

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

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)).

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

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

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)).

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

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)).

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

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)).

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)).

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).

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).

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)).

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

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

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

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

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).

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).

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)).

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).

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).

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).

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")).

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))).

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

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).

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).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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

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)).

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)).

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

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)).

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)).

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

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)).

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)).

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

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)).

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

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)).

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)).

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)).

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)).

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)).

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)).

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

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

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)).

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

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

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

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)).

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)).

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)).

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

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)).

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

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

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)).

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)).

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)).

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)).

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)).

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)).

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

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)).

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

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

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

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)).

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

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)).

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

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

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

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)).

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)).

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

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)).

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)).

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

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

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)).

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)).

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

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

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)).

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

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)).

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)).

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)).

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)).

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

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

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)).

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

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)).

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

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

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)).

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

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

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)).

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)).

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)).

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)).

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

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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)).

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).

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).

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).

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).

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).

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

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).

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

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

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).

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).

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).

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

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)).

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).

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)).

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).

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)).

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)).

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).

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)).

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)).

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).

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).

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).

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)).

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).

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).

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

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).

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)).

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)).

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)).

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)).

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)).

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)).

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).

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).

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)).

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).

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)).

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)).

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))).

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).

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).

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)).

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)).

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)).

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).

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).

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).

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)).

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)).

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)).

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)).

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).

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).

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).

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)).

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)).

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)).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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).

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

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

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).

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).

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).

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)).

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))).

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”)).

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)”)).

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)”)).

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)")).

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)).

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")).

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))).

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

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)).

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).

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).

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).

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).

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).

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)).

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).

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).

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)).

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)).

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))).

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)).

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).

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)).

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)).

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).

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)).

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)).

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)).

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)).

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).

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)).

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)).

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

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)).

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

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)).

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

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)).

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)).

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

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).

554. For example, on May 3, 2006, the LabMD server would not run a virus scan. (CX0035 (APT Service Invoice) at 2).

555. The servers' antivirus program did not automatically scan for viruses or perform regular scans between 2006 and 2009. (CX0735 (Kaloustian, IHT at 91)).

556. Between 2006 and 2009, antivirus was deployed only after a problem was observed. (CX0735 (Kaloustian, IHT at 91-92)).

557. LabMD did not have tools to monitor the network for viruses as of October 2006. (CX0735 (Kaloustian, IHT at 91)).

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)).

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)).

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)).

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)).

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)).

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)).

568. ClamWin was not managed centrally by a network administrator, and required individual updates to each computer. (CX0735 (Kaloustian, IHT at 126-32)).

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)).

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)).

571. LabMD's IT Department employees did not always update ClamWin virus definitions on employee computers. (CX0735 (Kaloustian, IHT at 130)).

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).

573. Yet LabMD relied on individual employees to update the virus definitions on their computers. (CX0735 (Kaloustian, IHT at 126-32)).

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)).

575. Many employee computers did not have Internet connections needed to update virus definitions on the computers. (CX0735 (Kaloustian, IHT at 160-61)).

576. Employee computers not connected to the Internet nonetheless could get viruses through CDs and thumb drives. (CX0735 (Kaloustian, IHT at 135-36)).

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)).

578. Many LabMD employees did not update their ClamWin antivirus virus definitions. (CX0735 (Kaloustian, IHT at 128)).

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)).

582. Between October 2006 and October 2009, AVG did not have a central reporting or management. (CX0734 (Simmons, IHT at 89)).

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)).

584. LabMD installed AVG antivirus on laptops. (CX0705-A (Bradley, Dep. at 82-83); CX0707 (Bureau, Dep. at 43, 45)).

585. The sales representatives' laptop computers could only automatically update programs when connected to the Internet. (CX0717 (Howard, Dep. at 91)).

586. Sales representatives could work offline. (CX0718 (Hudson, Dep. at 182)).

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)).

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)).

591. LabMD relied on individual employees to run scans on their computers. (CX0735 (Kaloustian, IHT at 129)).

592. LabMD did not have a policy requiring employees to run ClamWin scans. (CX0735 (Kaloustian, IHT at 130)).

593. LabMD did not verify that employees had run antivirus scans. (CX0735 (Kaloustian, IHT at 131)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

605. LabMD's IT employees only inspected employee computers when employees complained about the performance of their computers. (CX0734 (Simmons, IHT at 92-93)).

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)).

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)).

608. AVG did not have central logging capability. (CX0734 (Simmons, IHT at 99-100)).

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)).

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)).

613. LabMD did not control ClamWin updates on computers it supplied to physician-clients' offices. (CX0724 (Maire, Dep. at 96)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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).

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)).

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).

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).

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)).

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).

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)).

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)).

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)).

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).

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)).

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)).

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)).

646. LabMD did not systematically review the firewall's limited logs to detect attempted unauthorized network access. (*Infra* ¶¶ 647-648).

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)).

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)).

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)).

652. The Zywall firewall had no traffic monitoring features. (CX0731 (Truett, Dep. at 67)).

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)).

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)).

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)).

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)).

657. However, LabMD did not log activity on employee computers. (CX0717 (Howard, Dep. at 98-99)).

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).

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)).

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)).

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)).

664. Some of the verifications in Exhibit CX0169 could have been performed automatically rather than manually. (CX0705-A (Bradley, Dep. at 80-82)).

665. Automating these security verifications would require purchasing software rather than using "shareware." (CX0705-A (Bradley, Dep. at 79-81)).

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).

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)).

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)).

671. LabMD's manual inspections focused on quickly fixing performance problems on computers used by employees. (CX0734 (Simmons IHT at 79-84)).

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)).

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)).

674. Manual inspections of employee computers could take as long as several hours. (CX0705-A (Bradley Dep. at 77)).

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)).

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)).

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)).

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).

681. LabMD allegedly created a checklist for employees to use in the daily walkaround. (CX0482 (IT Dept Walkaround Checklist)).

682. The Walkaround Checklist, Exhibit CX0482, was not in use from October 2006 through August 2009. (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)).

684. No IT Department employee other than Mr. Hyer manually inspected LabMD computers between 2009 and 2012. (CX0719 (Hyer, Dep. at 99)).

685. Mr. Hyer kept no records of his manual inspections. (CX0719 (Hyer, Dep. at 99)).

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)).

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)).

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).

692. The LimeWire application installed on the computer used by LabMD's billing manager was not needed for business purposes. (Ans. ¶ 20).

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)).

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)).

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)).

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)).

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).

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).

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)).

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)).

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).

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)).

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)).

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).

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)).

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)).

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)).

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).

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).

716. Penetration tests have been available to IT practitioners since at least 1997. (CX0740 (Hill Report) ¶ 71).

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).

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).

719. IT practitioners use this information to identify risks early and address these vulnerabilities. (CX0740 (Hill Report) ¶¶ 70, 76).

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)).

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)).

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)).

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)).

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)).

725. LabMD did not conduct on its own any penetration tests equivalent to the ones that ProviDyn conducted. (CX0719 (Hyer, Dep. at 164)).

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)).

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)).

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).

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)).

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)).

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)).

734. On July 18, 2010, ProviDyn analyzed penetration tests on three LabMD servers, including Mapper. (CX0054 (July 2010 ProviDyn Network Security Scan-Mapper)).

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)).

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")).

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).

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).

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).

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).

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).

742. Level 1 (Low Risk) vulnerabilities are informational, such as open ports. (CX0070 (May 2010 ProviDyn Network Security Scan-Mapper) at 37).

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).

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)).

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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)).

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).

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).

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).

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).

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).

777. The CVE alert for this vulnerability, CVE-1999-0527, was released in 1999. **(**CX0054 (July 2010 ProviDyn Network Security Scan-Mapper) at 18).

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).

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

794. Wireshark is an example of a traffic capture or network sniffer tool. (CX0740 (Hill Report) ¶¶ 68(b), 71).

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

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)).

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)).

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)).

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).

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).

814. Companies can use operating system functionalities and other applications to limit employees’ access to information. (CX0740 (Hill Report) ¶ 85).

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).

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)).

819. Nothing prevented staff from accessing the information of patients for which they had no job-related need. (CX0706 (Brown, Dep. at 117-18)).

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)).

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)).

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).

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)).

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)).

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)).

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).

831. IT practitioners regularly purged unneeded data throughout the Relevant Time Period. (CX0740 (Hill Report) ¶ 80(b)).

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).

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).

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)).

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)).

838. LabMD imported data from legacy systems into the systems currently in use. (CX0443 (2/24/2010 Access Letter Response) at 6).

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)).

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)).

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)).

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).

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)).

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)).

847. LabMD maintained Personal Information on over 750,000 patients. (CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) at 5, Adm. 23).

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).

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)).

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)).

853. Proper training is integral to a reasonable layered data security strategy. (Hill, Tr. 169-70).

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).

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).

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).

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).

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).

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)).

862. LabMD’s IT contractor prior to March 2007, APT, did not provide security training. (CX0731 (Truett, Dep. at 125)).

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).

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)).

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).

868. Employees should also receive periodic training on acceptable use of computer equipment, current threats, and best practices. (CX0740 (Hill Report) ¶¶ 87, 89).

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)).

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).

873. Ms. Carmichael, a consultant who put LabMD's Compliance Program in place, developed compliance training for LabMD. (CX0708 (Carmichael, Dep. at 22-23)).

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).

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)).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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).

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)).

889. Mr. Hyer only provided training to IT employees Mr. Bradley and Ms. Parr, and the accounting manager. (CX0719 (Hyer, Dep. at 159-60)).

890. Mr. Hyer provided training to the LabMD accounting manager to help use IT to reduce her workload. (CX0719 (Hyer, Dep. at 160)).

891. None of training that Mr. Hyer provided to the accounting manager involved security issues. (CX0719 (Hyer, Dep. at 160-61)).

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).

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).

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).

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)).

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)).

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).

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)).

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).

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).

905. Usernames and passwords are a common authentication mechanism. (Hill, Tr. 176; CX0740 (Hill Report) ¶ 94).

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).

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).

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).

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)).

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).

913. Mr. Hyer stated that LabMD's passwords were "not as complex as they should have been." (CX0719 (Hyer, Dep. at 26-27)).

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).

915. Dictionary words are inherently weak passwords. (CX0740 (Hill Report) ¶ 87).

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).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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).

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)).

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)).

935. To ensure reasonable password policies are enforced, a company's password management should be centralized. (CX0740 (Hill Report) ¶ 94).

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).

937. The Windows operating system includes a centralized scheme to manage passwords. (CX0740 (Hill Report) ¶ 95(a)).

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)).

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)).

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)).

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).

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)).

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).

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)).

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)).

948. Ms. Brown's credentials were assigned to her by LabMD. (CX0706 (Brown, Dep. at 15)).

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)).

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)).

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)).

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).

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)).

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)).

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)).

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).

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)).

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)).

963. At least six employees used "LabMD" as a password. (CX0167 (PC Tracking (John) Spreadsheet); CX0705-A (Bradley, Dep. at 125-26)).

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)).

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).

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).

970. From October 2006 through April 2009, every server login username was "admin," and every password was "LABMD." (CX0735 (Kaloustian, IHT at 294-96)).

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)).

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).

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)).

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)).

977. LabMD would not reject any requested user credentials. (CX0728 (Randolph, Midtown Urology Designee, Dep. at 39-41)).

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)).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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).

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).

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).

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)).

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)).

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).

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).

999. Hackers exploit software bugs to gain unauthorized access to computer resources and data. (CX0740 (Hill Report) ¶ 99).

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)).

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).

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).

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).

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)).

1007. The support life-cycle for Windows NT 4.0 ended on June 30, 2004. (CX0740 (Hill Report) ¶ 100(c), 100(c) n.50).

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)).

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)).

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)).

1013. The LabNet server used Veritas backup software. (CX0724 (Maire Dep. Tr.) at 22-23; CX0735 (Kaloustian, IHT at 285-87)).

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).

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).

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)).

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)).

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).

1021. The updates that would have corrected this vulnerability would be available to LabMD at no cost. (Hill, Tr. 194).

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).

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).

1026. ProviDyn identified the "buffer overflow" vulnerability as a level 4, or "Critical Risk." (CX0067 (ProviDyn Network Security Scan – LabNet) at 22, 65).

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)).

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).

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).

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).

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).

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).

1035. This vulnerability provided hackers with access to specific information on the host, including security settings. (CX0740 (Hill Report) ¶ 100(e)).

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).

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).

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).

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).

1040. LabMD could have easily addressed this vulnerability by following instructions provided by Microsoft. (CX0737 (Hill Rebuttal Report) ¶ 29 n.45).

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)).

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).

1046. The process of detection enables the organization to identify and patch holes in its security system. (CX0740 (Hill Report) ¶ 103; Hill, Tr. 195).

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)).

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).

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).

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).

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).

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).

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).

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)).

1057. Sales representatives had administrative rights to their laptops, and were able to download software. (CX0722 (Knox, Dep. at 54-56)).

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)).

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).

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)).

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)).

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).

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)).

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)).

1067. Backups should not be stored on employee workstations. (CX0740 (Hill Report) ¶ 104(b)).

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)).

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).

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).

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).

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)).

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)).

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).

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)).

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).

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)).

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)).

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)).

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)).

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).

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)).

1087. As of October 2006, the software firewalls on LabMD's servers were disabled. (CX0735 (Kaloustian, IHT at 293-94)).

1088. Employee workstations should be configured to use a software firewall. (CX0740 (Hill Report) ¶ 104(f)).

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)).

1090. On August 25, 2004, Microsoft released Windows XP Service Pack 2, which included Windows Firewall. (CX0740 (Hill Report) ¶ 104(f)).

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)).

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).

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)).

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)).

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).

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).

1099. Firewall ports can be set up to block unwanted traffic. (Hill, Tr. 197-98).

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).

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).

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).

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).

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).

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).

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)).

1109. File Integrity Monitoring might have detected the LimeWire file-sharing application. (Hill, Tr. 199-201; CX0740 (Hill Report) ¶ 105(b)).

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)).

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).

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).

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)).

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)).

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))).

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).

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).

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).

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).

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).

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)).

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).

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)).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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)).

1154. IT practitioners regularly purged data from a network throughout the Relevant Time Period. (CX0740 (Hill Report) ¶ 80(b)).

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).

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).

1159. LabMD could have adequately trained employees to safeguard Personal Information at relatively low cost. (Hill, Tr. 173-76; CX0740 (Hill Report) ¶ 92).

1160. Several nationally recognized organizations provide low-cost and free IT security training courses. (Hill, Tr. 173-74; CX0740 (Hill Report) ¶ 89 & n.30).

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).

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).

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).

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)

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).

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).

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).

1172. These systems provide free notifications from vendors, as well as CERT, OSVDB, NIST, and others. (CX0740 (Hill Report) ¶ 99).

1173. Vendors such as Microsoft issue updates and patches to fix coding errors found in their software. (Hill, Tr. 105-06).

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)).

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)).

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).

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)).

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).

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)).

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)).

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)).

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)).

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)).

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).

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).

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).

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).

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).

1193. Peer-to-peer networks make available files that others can come and take. (CX0738 (Shields Rebuttal Report) ¶ 22).

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).

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).

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).

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).

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).

1201. A peer is a computer that is connected to the peer-to-peer network using a Gnutella client. (Shields, Tr. 827).

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).

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).

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).

1207. LimeWire was a popular Gnutella client. (Shields, Tr. 850).

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).

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).

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).

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).

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).

1215. Downloading is transferring a file from one computer to another. (Shields, Tr. 829).

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).

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).

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).

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).

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).

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).

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).

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)).

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)).

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)).

1228. Multiplying copies and multiplying users sharing them increases the likelihood that a sensitive file will be misused. (CX0721 (Johnson, Dep. at 100)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1242. In 2001, the search system changed to a protocol defined in the Gnutella 0.6 definition. (CX0738 (Shields Rebuttal Report) ¶ 25).

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).

1244. Ultrapeers are connected to a larger number of other ultrapeers. (CX0738 (Shields Rebuttal Report) ¶ 25).

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).

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).

1247. A peer is normally connected to about three ultrapeers. (Shields, Tr. 832).

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).

1249. Each ultrapeer will contact 32 other ultrapeers. (Shields, Tr. 833). Those ultrapeers will then send it on to other ultrapeers. (Shields, Tr. 833).

1250. The query will be forwarded for only a limited number of hops. (Shields, Tr. 846-47).

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).

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).

1253. The TTL field mechanism was designed to prevent queries from taking over the Gnutella network. (Shields, Tr. 846-47).

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).

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).

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).

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)).

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).

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).

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)).

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)).

1264. Searches also cover only a portion of the network. (Shields, Tr. 847; CX0738 (Shields Rebuttal Report) ¶ 27).

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).

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).

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).

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).

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).

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).

1275. Identity thieves search for files to aggregate large amounts of personal data for use or resale. (Wallace, Tr. 1376-77, 1380-81).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1305. Crawling the Gnutella network is a common enough activity that it has its own Wikipedia page. (CX0738 (Shields Rebuttal Report) ¶ 95).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1332. US-CERT is known as an expert on security threats and as a resource of information about those threats. (Shields, Tr. 887).

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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).

1357. The 1718 File was created and stored on a LabMD computer. (Daugherty, Tr. 1078-79).

1358. The 1718 File is a billing file from the Lytec system. (CX0709 (Daugherty, Dep. at 146); CX0736 (Daugherty, IHT at 83-84)).

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)).

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)).

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).

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)).

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)).

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).

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)).

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))

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)).

1371. LabMD had no business need for LimeWire on the Billing Computer. (Ans. ¶ 20; CX0716 (Harris, Dep. at 146)).

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)).

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).

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).

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).

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).

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).

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)).

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)).

1384. Prior to the 2008 incident, other employees were aware that Ms. Woodson had LimeWire on her workstation. (CX0716 (Harris, Dep. at 86)).

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)).

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)).

1387. Ms. Woodson created music CDs at LabMD and gave them to other employees. (CX0716 (Harris, Dep. at 89)).

1388. Ms. Woodson made the CDs through LimeWire by downloading music to her computer. (CX0716 (Harris, Dep. at 89)).

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)).

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)).

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)).

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).

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).

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).

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)).

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)).

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)).

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)).

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).

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)).

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)).

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).

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).

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).

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).

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).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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).

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).

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)).

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)).

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)).

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).

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).

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).

1442. The handwritten notations on pages 4, 7, and 9 of CX0088 were Social Security numbers. (CX0720 (Jestes, Dep. at 35-36)).

1443. The handwritten notations on pages 1, 5, and 8 of CX0088 were monetary amounts, and a phone number. (CX0720 (Jestes, Dep. at 36)).

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)).

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)).

1448. Detective Jestes believed that the computers might have evidentiary value. (CX0720 (Jestes, Dep. at 37-38)).

1449. The seized computers, a desktop and a laptop, were subsequently examined by Detective Shim of the SPD. (CX0720 (Jestes, Dep. at 37-39)).

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)).

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)).

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)).

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)).

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)).

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)).

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)).

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).

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).

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)).

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).

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)).

1466. The number was active through December 2013. (CX0710-A (Daugherty, LabMD Designee, Dep. at 76)).

1467. LabMD does not know how many people called the number in response to the letter. (CX0710-A (Daugherty, LabMD Designee, Dep. at 78)).

1468. LabMD did not hire a call center. (CX0710-A (Daugherty, LabMD Designee, Dep. at 76)).

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).

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).

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).

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).

1475. "Identity theft" is also sometimes referred to as "identity fraud." (Van Dyke, Tr. 577; CX0741 (Van Dyke Report) at 3).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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)).

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).

1529. Victims of ENCF fall prey to crimes that total over $1,805 on average. (CX0741 (Van Dyke Report) at 97).

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).

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).

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).

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).

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).

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).

1540. Consumers who are victims of ECF fall prey to crimes that total over $1,373 on average. (CX0741 (Van Dyke Report) at 9).

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)).

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).

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).

1547. A victim of identity theft may have to clean up multiple fraudulent accounts. (Kam, Tr. 394-95; CX0742 (Kam Report) at 13).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1561. The delay in receiving the refund can extend to be as long as six months. (CX0742 (Kam Report) at 14).

1562. The delay in receiving the refund materially impacts consumer victims' cash flow. (CX0742 (Kam Report) at 14).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1588. In 2011, 1 in 5 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

1589. In 2012, 1 in 4 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

1590. In 2013, 1 in 3 Americans suffered identity fraud in the last 12 months. (CX0741 (Van Dyke Report) at 7).

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).

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)).

1595. Health insurance policy information and SSNs can be used to commit medical identity frauds. CX0741 (Van Dyke Report) at 13).

1596. Medical identity theft is a serious problem. (CX0742 (Kam Report) at 12).

1597. Medical identity theft affects an estimated 1.84 million Americans. (CX0742 (Kam Report) at 12).

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).

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).

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).

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).

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).

1607. Consumers can suffer when information disclosing that they have a stigmatized condition is disclosed. (Kam, Tr. 447-48; CX0742 (Kam Report) at 16).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

1635. In 2012, 355,425 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 13, 14).

1636. In 2011, 449,462 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

1637. In 2010, 426,026 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

1638. In 2009, 824,581 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

1639. In 2008, 567,484 consumers had their information misused to obtain medical services. (CX0741 (Van Dyke Report) at 14).

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).

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).

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).

1647. Cyber criminals are targeting healthcare organizations because of the high value of sensitive medical information. (Kam, Tr. 519; CX0742 (Kam Report) at 23).

1648. Organizations with inadequate data security programs are vulnerable to unauthorized disclosures of sensitive Personal Information. (CX0742 (Kam Report) at 23).

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).

1650. The consumer PII maintained by LabMD is a target of data thieves. (CX0741 (Van Dyke Report) at 12).

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).

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).

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).

1656. There is a risk of harm to consumers when a company fails to protect sensitive Personal Information. (CX0742 (Kam Report) at 10).

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).

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).

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)).

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)).

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)).

1664. An unauthorized disclosure of the 1718 File was made in May 2008. (JX0001-A (Joint Stips. of Law, Fact, and Authenticity) at 4).

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).

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).

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).

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).

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).

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)).

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).

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)).

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).

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).

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).

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).

1685. Several of the CPT codes in the 1718 File indicate tests for sensitive conditions. (Kam, Tr. 447-49; CX0742 (Kam Report) at 21).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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).

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.

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).

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)).

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).

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).

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).

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)).

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).

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)).

1716. The "Name" column on LabMD's Day Sheets is the patient's name. (CX0733 (Boyle, IHT at 53)).

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)).

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).

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).

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)).

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)).

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)[2]).

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).

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).

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).

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).

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).

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).

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).

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).

[2] 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.

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).

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).

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).

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).

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).

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).

1743. There are 43 anticipated cases of NAF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

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).

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).

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).

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).

1750. There are 43 anticipated cases of ENCF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

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).

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).

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).

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).

1757. There are 79 anticipated cases of ECF due to the unauthorized disclosure of the Sacramento Day Sheets. (CX0741 (Van Dyke Report) at 12).

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).

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).

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).

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).

1764. Notification does not eliminate the risk of harm from identity crime to consumers. (Kam, Tr. 420; CX0742 (Kam Report) at 17).

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).

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)).

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).

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).

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).

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).

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).

1778. SUN did not inform consumers that their specimens were going to be tested by LabMD. (CX0726 (Maxey, SUN Designee, Dep. at 78)).

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)).

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)).

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)).

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)).

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).

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)).

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)).

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)).

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)).

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)).

1795. Sales representatives' assurances about security were based on what they were told in their sales and management training. (CX0718 (Hudson, Dep. at 68)).

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)).

1799. Intentionally left blank.

1. COMPLAINT COUNSEL'S PROPOSED CONCLUSIONS OF LAW

1.1 Burden of Proof

1. Rule 3.43(a) states that "Counsel representing the Commission . . . shall have the burden of proof," except as to a factual propositions put forward by another proponent, such as affirmative defenses. 16 C.F.R. § 3.43; *see also* Administrative Procedure Act, 5 U.S.C. § 556(d); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2).

2. The standard of proof is preponderance of the evidence. *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *134-35 (Aug. 5, 2009) (collecting cases); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2-3).

3. Complaint Counsel has the burden of proof to prove by a preponderance of the evidence that LabMD's practices are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 3).

4. Intentionally left blank.

1.2 Jurisdiction

5. Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). The act defines "commerce" as, *inter alia*, "commerce among the several States." *Id*. § 44.

6. Respondent has engaged in "commerce," as defined in the FTC Act. JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2. Respondent has admitted that it tested samples from numerous states, including Alabama, Mississippi, Florida, Georgia, Missouri, Louisiana, and Arizona. Ans. ¶ 5; CX0766 (LabMD's Resps. and Objs. To Reqs. For Adm.) at 3, Adm. 8-12. Furthermore, the consumers whose samples Respondent tested and from whom Respondents collects payments are "located throughout the United States." CX0766 (LabMD's Resps. and Objs. To Reqs. For Adm.) at 3, Adms. 9-12; CX0088 (*in camera*) (LabMD Copied Checks) at 1-10; CX0726 (Maxey, SUN Designee, Dep. at 17-31); CX0718 (Hudson, Dep. at 131-33); CX0722 (Knox, Dep. at 19); CX0706 (Brown, Dep. at 146-47); CX0715-A (Gilbreth, Dep. at 6); CX0713-A (Gardner, Dep. at 27-29); CX0714-A ([Fmr. LabMD Empl.], Dep. at 35-36). Respondent's practices are thus "in or affecting commerce." *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 17 (rejecting Respondent's "frivolous" argument that its conduct does not meet the definition of "commerce" based on allegation that it tested samples from consumers throughout the United States and Respondent's admission that LabMD test samples sent from six states outside of Georgia); *see also P.F. Collier & Son Corp. v. FTC*, 427 F.2d 261, 272 (6th Cir. 1970) (holding that the nationwide scopes of operations imparted the requisite interstate character).

7. The Commission has jurisdiction over persons, partnerships, and corporations. 15 U.S.C. § 45(a)(2). A "corporation" is defined in Section 4 of the FTC Act as "any company . . .

which is organized to carry on business for its own profit or that of its members[.]" 15 U.S.C. § 44. LabMD is a privately-held corporation organized under the laws of the state of Georgia. *Supra* CCFF § 4.2 (Corporate Structure) (¶¶ 54-55). The Commission has jurisdiction over LabMD, a corporation.

8. Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1).

9. The Commission's authority to take action against unfair acts or practices ("unfairness") under Section 5 of the FTC Act extends to unreasonable data security practices. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 2 ("LabMD's Motion to Dismiss . . . calls on the Commission to decide whether the FTC Act's prohibition of 'unfair . . . acts or practices' applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does."); *FTC v. Wyndham Worldwide Corp.*, 2014 WL 1349019 at *6-9 (D.N.J. Apr. 7, 2014) (concluding that Section 5 authority extends to data security).

10. LabMD's unreasonable data security practices constitute unfair acts or practices within the scope of Section 5 of the FTC Act, 15 U.S.C. § 45.

11. Intentionally left blank.

1.3 LabMD's Failure to Employ Reasonable Measures to Prevent Unauthorized Access to Personal Information Was, and Is, an Unfair Practice

12. An unfair practice is defined as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n); JX0001-A (Joint Stips. of Fact, Law, & Auth.) at 2).

13. Congress deliberately delegated broad power to the FTC under Section 5 of the FTC Act to address unanticipated practices in a changing economy. *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985); *see also* Comm'n Order Denying Resp't's Mot. to Dismiss at 6 (Jan. 16, 2014) (finding no evidence of "congressional intent to preserve inadequate data security practices that unreasonably injure consumers").

14. The codification of unfairness established a cost-benefit analysis to evaluate whether practices are unfair. *See* 15 U.S.C. § 45(n) (requiring evaluation of the likelihood of "substantial injury" and of "countervailing benefits"); J. Howard Beales III, Director, Bureau of Consumer Protection, Federal Trade Comm'n Remarks at the Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) ("[C]odification of those principles in 1994 re-established a cost/benefit analysis (injury to consumers not outweighed by countervailing benefits) as the test for unfairness.").

15. As the Commission recently expressed it: "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be

reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of the available tools to improve security and reduce vulnerabilities." Comm'n Statement Marking 50th Data Sec. Settlement (Jan 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

16. As with the application of the reasonableness standard of care in any other circumstance, what constitutes reasonable data security practices for a company that maintains consumers' sensitive Personal Information will vary depending on the circumstances. *See FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) ("[T]he proscriptions in [Section] 5 are flexible, 'to be defined with particularity by the myriad of cases from the field of business.'") (internal citations omitted); *Brock v. Teamsters Local Union No. 863*, 113 F.R.D. 32, 34 (D.N.J. 1986) (reasonableness under prudent man standard "tried on the individual facts of [the] case" in light of standards developed in case law); *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3-4 (D. Nev. Sept. 9, 2013) (applying "reasonable and prudent person" standard in negligence case for failure to safeguard electronically held data). Reasonableness turns on the amount and sensitivity of the information the company handles (going to the magnitude of injury from unauthorized access to information) and the nature and scope of the firm's activities (going to the structure of the firm's network, how the network operates, the types of security vulnerabilities and risks it faces, and feasible protections). *Cf. FTC v Accusearch, Inc.*, 2007 WL 4356786 at *7 (D. Wyo. Sept. 28, 2007) (defendants "can reasonably be expected to know" the legal environment in which their industries operate).

17. A company can reference the recommendations of government agencies, such as the National Institute of Standards and Technology ("NIST"), well-known private sources, such as the SANS Institute and other information technology training institutes, and manufacturers of the software and hardware the company uses for guidance on how to identify the risks and vulnerabilities they face, and select and maintain data security practices that are reasonable under their circumstances. *See* CX0740 (Hill Report) ¶¶ 60 & n.8, 74; Shields, Tr. 884-85; CX0738 (Shields Rebuttal Report) ¶ 40; *supra* CCFF § 6.2 (Comprehensive Information Security Program) (¶¶ 1121-1124). NIST, for example, has published materials on a wide variety of information security topics, including basic security practices and risk assessment methods that can be tailored to the circumstances. *See* CX0740 (Hill Report) ¶ 74 & n.25. Similarly, the SANS Institute has since 2001 annually published and updated a free, easily accessible list of the most critical security vulnerabilities confronting firms, security professionals, and law enforcement. The compilation includes reference materials, information about new vulnerabilities, security measures that companies may use to defend against attacks, and links to free security tools. *See* CX0740 (Hill Report) at 64.

18. Companies may also review FTC complaints and consent decrees. *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *15 (D.N.J. Apr. 7, 2014) (noting that consent orders provide guidance to courts and litigants); *see also* Comm'n Order Denying Resp't's Mot. to Dismiss at 14 ("Complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings."); *In re TJX*

Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496-97 (1st Cir. 2009) (in reviewing data security claim under state unfair practices act, noting that "a substantial body of FTC complaints and consent decrees focus on" data security and provide interpretive guidance for determining unfair conduct).

19. The FTC's consent decrees illustrate commonly-known data security issues, highlight security vulnerabilities similar to those found with respect to LabMD, and provide notice about some of the types of data security practices the FTC has identified as unreasonable. They concern fundamental security elements, including: conducting risk assessments to identify reasonably foreseeable risks; assessing the effectiveness of existing security measures and adopting additional measures in light thereof; testing and monitoring security measures for effectiveness; and adjusting the measures appropriately. For example, the complaints in a number of FTC actions allege that the respondent failed to conduct adequate risk assessments and, as a result, failed to adopt easily implemented measures to address reasonably foreseeable risks that an appropriate risk assessment would have revealed. *See, e.g.*, *BJ's Wholesale Club, Inc.*, FTC File No. 042-3160, Docket No. C-4148 (2005) (alleging unfair failure to employ reasonable security measures, including failing to conduct security investigations); *DSW, Inc.*, FTC File No. 052-3096, Docket No. C-4157 (2006) (alleging unfair failure to employ reasonable security measures, including failing to employ sufficient measures to detect unauthorized access); *Nations Title Agency, Inc.*, FTC File No. 052-3117, Docket No. C-4161 (2006) (alleging unfair failure to employ reasonable security measures, including failure to assess risks to consumer information it collected and stored and failure to implement policies and procedures in key areas); *CardSystems Solutions, Inc.*, FTC File No. 052-3148, Docket No. C-4168 (2006) (alleging unfair failure to employ reasonable security measures, including failing to adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks); *Reed Elsevier, Inc.*, FTC File No. 052-3094, Docket No. C-4226 (2008) (alleging unfair failure to employ reasonable security measures, including allegations related to insecure user credentials to access Personal Information of consumers); *TJX Cos., Inc.*, FTC File No. 072-3055, Docket No. C-4227 (2008) (alleging unfair failure to employ reasonable security measures, including allegations relating to insecure user credentials and failure to employ sufficient measures to detect and prevent unauthorized access to computer networks); *CVS Caremark Corp.*, FTC File No. 072-3119, Docket No. C-4259 (2009) (alleging unfair failure to employ reasonable security measures, including failure to train employees to treat information securely and failure to implement a reasonable process for discovering and remedying risks to Personal Information); *Dave & Buster's, Inc.*, FTC File No. 082-3153, Docket No. C-4291 (2010) (alleging unfair failure to employ reasonable security measures, including failure to detect and prevent unauthorized access to computer networks or conduct security investigations); *Rite Aid Corp.*, FTC File No. 072-3121, Docket No. C-4308 (2010) (alleging unfair failure to employ reasonable security measures, including failure to properly train employees); *Fajilan & Assocs.*, FTC File No. 092-3089, Docket No. C-4332 (2011) (alleging unfair failure to employ reasonable security measures, including failure to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *ACRAnet, Inc.*, FTC File No. 092-3088, Docket No. C-4331 (2011) (alleging unfair failure to employ reasonable security measures, including failure

to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *SettlementOne Credit Corp.*, FTC File No. 082-3208, Docket No. C-440 (2011) (alleging unfair failure to employ reasonable security measures, including failure to develop and disseminate information security policies, perform risk assessments, address risks identified in risk assessments, and monitor compliance); *Ceridian Corp.*, FTC File No. 102-3160, Docket No. C-4325 (2011) (alleging unfair failure to adequately assess the vulnerability of its network to commonly known or reasonably foreseeable attacks and failure to employ reasonable measures to detect or prevent unauthorized access to Personal Information); *Lookout Servs., Inc.*, FTC File No. 102-3076, Docket No. C-4326 (2011) (alleging unfair failure to implement reasonable policies and procedures for the security of sensitive consumer information and allegations relating to insecure user credentials); *Upromise, Inc.*, FTC File No. 102-3116, Docket No. C-4351 (2012) (alleging unfair failure to assess and address risks to consumer information); *EPN, Inc.*, FTC File No. 112-3143, Docket No. C-4370 (2012) (alleging unfair failure to adopt an appropriate information security program; assess risks to Personal Information; adequately train employees; and use reasonable methods to prevent, detect, and investigate unauthorized access to Personal Information); *Franklin's Budget Car Sales, Inc.*, FTC File No. 102-3094, Docket No. C-4371 (2012) (alleging unfair failure to adopt an appropriate information security program; assess risks to Personal Information; adequately train employees; and use reasonable methods to prevent, detect, and investigate unauthorized access to Personal Information); *Compete, Inc.*, FTC File No. 102-3155, Docket No. C-4384 (2012) (alleging unfair failure to design and implement reasonable information safeguards and use readily-available, low-cost measures to assess and address risks); *HTC Am., Inc.*, FTC File No. 122-3049, Docket No. C-4406 (2013) (alleging unfair failure to implement adequate security and privacy guidance and training for its staff; conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities; and follow well-known and commonly-accepted security practices in its industry).

20. The consent decrees approved by the Commission in data security matters all provide the same basic guidance by imposing relief that requires respondents to implement a comprehensive information security plan that includes the same fundamental security elements as required by the notice order. The consent decrees require a respondent to establish a comprehensive information security program with elements that (1) designate an employee or employees to coordinate and be accountable for the information security program; (2) identify risks to the security, confidentiality, and integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks; (3) design and implement reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures; (4) develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and require service providers by contract to implement and maintain appropriate safeguards; and (5) evaluate and adjust the information security program in light of the testing and monitoring required by subpart (3), any material changes to respondents' operations or business arrangements, and any other circumstances that respondent knows or has reason

to know may have a material impact on effectiveness of its information security program. The orders provide further guidance on subpart (2), risk identification, requiring respondents to assess risks in each area of relevant operation, including but not limited to (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other system failures. *See generally* cases cited in Conclusion of Law ¶ 19, *supra*.

21. Complaint Counsel has demonstrated by a preponderance of the evidence that: (1) LabMD's data security failures caused or are likely to cause substantial injury to consumers, (2) consumers cannot reasonably avoid the substantial injury caused or likely to be caused by LabMD's data security failures, and (3) LabMD's data security failures are not outweighed by countervailing benefits to consumers or to competition. LabMD, therefore, has violated Section 5 of the FTC Act. *See* 15 U.S.C. § 45(n).

22. The order against LabMD proposed by Complaint Counsel is appropriate as a result of the company's violations of Section 5.

23. Intentionally left blank.

1.3.1 LabMD's Data Security Failures Caused or are Likely to Cause Substantial Injury to Consumers

1.3.1.1 Caused or Likely to Cause

24. A showing of substantial injury or the likelihood of substantial injury from the unauthorized disclosure of Personal Information does not require that an actual breach occur. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 19 ("[O]ccurences of actual data security breaches or 'actual, completed economic harms' are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted 'unfair…acts or practices.'") (citations omitted); *cf. FTC v. Toysmart.com LLC*, No. 00-11341 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/sites/default/files/documents/cases/toysmartconsent.htm (consent order) (declining to wait for bankrupt company that intended to sell consumers' Personal Information in violation of its privacy policy representations to complete the planned sale before providing relief).

25. Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury. The inquiry turns on whether any potential or actual unauthorized disclosure of Personal Information held by a company due to unreasonable data security practices caused or is likely to cause consumer harm. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 18-19 (requiring assessment of whether a company's "data security procedures were 'unreasonable' in light of the circumstances"); *see also, e.g.*, Statement of Basis and Purpose, Debt Settlement Amendments to Telemarketing Sales Rule, 75 Fed. Reg. 48458, 48482, n. 334 (Aug. 10, 2010) (stating that while in rulemaking proceeding there was evidence that the collection of advance fees causes actual harm, the Section 5 unfairness standard does not require the Commission to "demonstrate *actual* consumer injury, but

only the *likelihood* of substantial injury") (emphasis original)); *cf. Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at *11-12 (7th Cir. July 20, 2015) (finding injury sufficient to satisfy Article III standing requirements because "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur" (quoting *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013)).

26. Likelihood of harm satisfies the unfairness analysis. *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *89 n.52 (1984) (rejecting dissent's assertion that the Commission was requiring actual harm rather than likelihood of harm, stating "[t]he ultimate question at issue is, indeed, risk. What is the risk of consumer harm?"); *see also id.* at n.45 (noting that while not usual, the reference to "risk" in the Unfairness Statement's discussion of an unfairness case involving health and safety risks "makes clear [that] unfairness cases may also be brought on the basis of likely rather than actual injury").

27. Failure to maintain adequate data security for Personal Information is likely to cause consumers substantial harm. Kam, Tr. 463-64 (opining that LabMD's failure to provide reasonable security increased the risk of unauthorized disclosure of the information it maintains.); CX0742 (Kam Report) at 23 (LabMD's failure to provide reasonable security for sensitive information it maintains created "an elevated risk of unauthorized disclosure of this information."); CX0741 (Van Dyke Report) at 3, 6 (reaching opinion that LabMD's unreasonable security placed consumers at significantly higher risk of becoming victims of identity theft); Van Dyke, Tr. 589 (stating that there is a correlation between exposure of consumer information and identity theft); CX0741 (Van Dyke) at 8 (demonstrating correlation between data breaches and identity theft).

28. Intentionally left blank.

1.3.1.2 Substantial Injury

29. A practice is unfair if it causes or is likely to cause "a small amount of harm to a large number of people, or if it raises a significant risk of concrete harm." *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *101 n.12 (1984) (Unfairness Statement).

30. In potentially exposing the Personal Information of 750,000 consumers to unauthorized disclosure, LabMD's data security failures are likely to cause injury to a large number of consumers.

31. Commission action is appropriate where, inter alia, "no private suit would be brought to stop the unfair conduct, since the loss to each of the individuals affected is too small to warrant it." *FTC v. Klesner*, 280 U.S. 19, 28 (1929).

32. Monetary harm exemplifies the injury prong of the unfairness standard. *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *97 (1984).

33. LabMD's data security failures are likely to cause consumers monetary harm from existing card fraud, existing non-card fraud, new account fraud, tax fraud, and medical

identity theft. *See generally* CCFF § 9 LabMD's Data Security Practices Caused or are Likely to Cause Substantial Injury to Consumers that is Not Reasonably Avoidable by the Consumers Themselves.

34. The entirety of harms likely to be caused by an unfair act or practice need not be monetarily quantifiable. *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988) (affirming Commission grant of summary judgment where injury included in part "intangible loss" relating to certainty of contract terms).

35. Defendant's acts or practices also cause substantial harm when consumers must spend "a considerable amount of time and resources" remediating problems caused by the defendant's conduct, such as closing compromised bank accounts. *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115-16 (S.D. Cal. 2008) (basing finding of substantial harm in part on "the cost of account holders' time" where defendants' practices compromised bank account security); *see also Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at *9 (7th Cir. July 20, 2015) (observing in a data breach involving credit cards, "there are identifiable costs associated with the process of sorting things out"), *13-14 (lost time and money spent by consumers protecting themselves from future identity theft "easily qualifies as a concrete injury"), *21 (finding that mitigation expenses and future injury are judicially redressable); *FTC v. Kennedy,* 574 F. Supp. 2d 714, 721 (S.D. Tex. 2008) (finding substantial injury where, *inter alia*, "consumers were forced to expend substantial time and effort" seeking refunds and other remediation of the defendant's unfair conduct).

36. LabMD's data security failures are likely to cause consumers substantial harm in the form of time spent remediating problems from new account fraud, existing non-card fraud, existing card fraud, and medical identity theft. *See generally supra* CCFF § 9 (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) *et seq.* (¶¶ 1472-1798)).

37. "Unwarranted health and safety risks may also support a finding of unfairness." *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *97 (1984) (Unfairness Statement). Indeed, the seminal unfairness case involved a product that caused physical injury to some consumers and was likely to harm more. *Int'l Harvester Co.*, 1984 WL 565290 at *90 & n.57.

38. LabMD's data security failures are likely to cause consumers substantial harm in the form of health and safety risks caused by medical identity theft. *Supra* CCFF §§ 9.1.2.3.1 (Integrity of Consumer Health Records Compromised Due to Medical Identity Theft Causes of Risk of Physical Harm to Consumers) (¶¶ 1612-1618), 9.3.4 (Impact on Consumers From Medical Identity Theft Stemming From Unauthorized Disclosure of the 1718 File) (¶¶ 1678-1681).

39. Loss of privacy can result in a "host of emotional harms that are substantial and real and cannot fairly be classified as either trivial or speculative." *FTC v Accusearch, Inc.*, 2007 WL 4356786 at *8 (D. Wyo. Sept. 28, 2007).

40. The disclosure of sensitive medical information, resulting in the loss of consumer privacy, constitutes substantial injury. Kam, Tr. 395-96; *see also* Kam, Tr. 445-53 (exposure of 1718 File was likely to lead to reputational harm to consumers based on the release of sensitive information about medical tests performed on consumers); CX0742 (Kam Report) at 16, 21 (victims who may have cancer or sexually transmitted diseases are particularly vulnerable to reputational harm).

41. Intentionally left blank.

1.3.2 Consumers Cannot Reasonably Avoid the Substantial Injury Caused or Likely to Be Caused by LabMD's Data Security Failures

42. Consumers have no way to discover LabMD's unreasonable security practices, and in many cases do not know to what laboratory their specimen is sent for analysis. *Supra* CCFF § 9.5.1.1.1 (Consumers Did Not Know LabMD Would Test Their Specimen and Receive Their Personal Information) (¶¶ 1777-1782); *see FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1112 (S.D. Cal. 2008) (consumers could not reasonably avoid injury where, inter alia, they "had never requested goods or services" from defendant).

43. Where consumers do not have a free and informed choice, injury is not reasonably avoidable. *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168-69 (9th Cir. 2012) ("In determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice." (quoting *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010)). An injury is reasonably avoidable if consumers "'have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end.'" *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (quoting *In re Orkin Exterminating Co.*, 108 F.T.C. 341, 366 (1986)).

44. Even where consumers know they are transacting with a particular company, they cannot always know the company's security practices in order to avoid injury at the hands of a company with unreasonable security practices. *Am. Fin. Svcs Ass'n v. FTC*, 767 F.2d 957, 976 (D.C. Cir. 1985) ("[C]ertain types of seller conduct or market imperfections may unjustifiably hinder consumers' free market decisions and prevent the forces of supply and demand from maximizing benefits and minimizing costs."); *see also BJ's Wholesale Club, Inc.*, FTC File No. 042-3160, Docket No. C-4148 (2005); *DSW, Inc.*, FTC File No. 052-3096, Docket No. C-4157 (2006); *TJX Cos., Inc.*, FTC File No. 072-3055, Docket No. C-4227 (2008); *CVS Caremark Corp.*, FTC File No. 072-3119, Docket No. C-4259 (2009); *Dave & Buster's, Inc.*, FTC File No. 082-3153, Docket No. C-4291 (2010); *Rite Aid Corp.*, FTC File No. 072-3121, Docket No. C-4308 (2010); *Upromise, Inc.*, FTC File No. 102-3116, Docket No. C-4351 (2012); *EPN, Inc.*, FTC File No. 112-3143, Docket No. C-4370 (2012); *Franklin's Budget Car Sales, Inc.*, FTC File No. 102-3094, Docket No. C-4371 (2012); *Compete, Inc.*, FTC File No. 102-3155, Docket No. C-4384 (2012); *HTC Am., Inc.*, FTC File No. 122-3049, Docket No. C-4406 (2013).

45. Intentionally left blank.

1.3.3 LabMD's Data Security Failures are Not Outweighed by Countervailing Benefits to Consumers or to Competition

46. "'[W]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition,'" the countervailing benefits prong of the unfairness test is "easily satisfied." *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (quoting *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal 2000)).

47. Where consumers do not knowingly purchase a product or service, there are unlikely to be countervailing benefits to a company's unfair practices. *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (finding no countervailing benefits where consumers "did not give their consent to enrollment in OnlineSupplier, and thus, the harm resulted from a practice for which they did not bargain"). Consumers whose laboratory work was sent to LabMD often did not have a choice in which lab was used. *Supra* § 9.5.1.1.1 (Consumers Did Not Know LabMD Would Test Their Specimen and Receive Their Personal Information) (¶¶ 1777-1782).

48. Countervailing benefits are determined based on the specific practice at issue in a complaint, not the overall operation of a business. *FTC v. Accusearch, Inc.*, 2007 WL 4356786 at *8 (D. Wyo. Sept. 28, 2007), judgment aff'd *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009) ("While there may be countervailing benefits to some of the information and services provided by 'data brokers' such as *Abika.com*, there are no countervailing benefits to consumers or competition derived from the specific practice of illicitly obtaining and selling confidential consumer phone records." (emphasis original)); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988) (upholding Commission finding of no countervailing benefits because an increase in fees "was not accompanied" by an increased level or quality of service); *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 2 (Jan. 15, 2014) (reiterating that countervailing benefit determination is made by "compar[ing] that harm to any benefits from that particular practice").

49. Consumers "realized no benefit" from LabMD's data security failures. *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *90 (1984).

50. Countervailing benefits are unlikely to be significant when more effective security measures could have been implemented at relatively low cost. *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *97 (1984) (Unfairness Statement) (stating that "[m]ost business practices entail a mixture of economic and other costs and benefits for purchasers" and framing the evaluation as to whether a practice is "injurious in its net effects," taking into account the "various costs that a remedy would entail").

51. LabMD could have discovered and corrected its security failures at low or no cost. *Supra* CCFF § 6 (LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures) *et seq.* (¶¶ 1113-1185); *see also Int'l Harvester Co.*, 104 FTC

949, 1984 WL 565290 at *91 (1984) ("Harvester's expenses were not large in relation to the injuries that could have been avoided.").

52. Because they could have been discovered and corrected at low cost, LabMD's data security failures did not provide any advantage over competing laboratories' practices. *See FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (where business model incorporating unfair acts and practices provides no advantage in the marketplace, "any benefits were small").

53. Because LabMD could have discovered and corrected its security failures at low or no cost, its data security failures provide no countervailing benefit to consumers or competition. *See Int'l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at *90 (1984) (identifying the "principal tradeoff to be considered" as "compliance costs").

54. Intentionally left blank.

1.4 Remedy

1.4.1 Corporate Liability

55. The Commission may enter an order against a corporation for violations of the FTC Act. 15 U.S.C. § 45(b).

56. Intentionally left blank.

1.4.2 Entry of the Notice Order is Appropriate and Necessary

57. Entering an order to require LabMD to implement reasonable data security for consumer Personal Information and to obtain biennial assessments is appropriate because the findings of fact are "supported by substantial evidence upon the record as a whole." *Niresk Indus. Inc. v. FTC,* 278 F.2d 337, 340 (7th Cir. 1960) (citation omitted).

58. An appropriate order must bear a reasonable relationship to the unlawful acts or practices alleged in the complaint. *See, e.g., FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 394-95 (1965); *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952); *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946). Within that framework, the Commission has "considerable discretion in fashioning an appropriate remedial order," *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *275, including an order to cease and desist from conduct found to violate Section 5 of the FTC Act. 15 U.S.C. § 45(b); *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 428 (1957).

59. The FTC has wide latitude in crafting appropriate relief. The Commission "cannot be required to confine its road block to the narrow lane the transgressor traveled; it must be allowed effectively to close all roads to the prohibited goal, so that its order may not be by-passed with impunity." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952).

60. LabMD has no intent to dissolve as a Georgia corporation. (JX0001-A (Joint Stips. of Law, Fact, and Auth.) at 3).

61. In the future, LabMD intends to employ the same policies and procedures to information in its possession as it employed in the past. (CX0765 (LabMD's Resps. to Second Set of Discovery) at 5-6 (Resp. to Req. 38), 7 (Resp. to Interrog. 12).

62. LabMD retains the Personal Information of over 750,000 consumers. *Supra* CCFF § 4.6.1 (Amount of Personal Information Collected) (¶ 78).

63. LabMD continues to operate a computer network consisting of switches, routers, servers, workstation computers, printers, a scanner, and an Internet connection at Mr. Daugherty's residence, as well as a workstation at a condominium that can remotely connect to a server at the private residence network and a printer for the condominium workstation. *Supra* CCFF § 4.7.4 (Internal Network from January 2014 to Present) (¶¶ 251-260).

64. LabMD continues to provide past test results to healthcare providers and continues to collect on monies owed to it. *Supra* CCFF § 4.4 (Wind Down and Current Status) (¶ 63).

65. Even if LabMD were not currently operating, it would not be a bar to entry of a notice order. *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953) (burden of proving that a case has become moot by reason of discontinuance of defendant's conduct is "a heavy one" that requires the defendant to demonstrate "'there is no reasonable expectation that the wrong will be repeated'" (citing *U.S. v. Alumunum Co. of Am.*, 148 F.2d 416, 448 (2d Cir. 1945)); *see also id.* at 632 ("The courts have rightly refused to grand defendants such a powerful weapon [procuring mootness by ceasing challenged conduct] against public law enforcement.").

66. As of February 2014, the paper records kept at Mr. Daugherty's residence were observed located in rooms throughout the house and were not secured in any way. (CX0725-A (Martin, Dep. at 22)).

67. Likewise, the patient specimens in the basement were also not secured in any way. (CX0725-A (Martin, Dep. at 23)).

68. As of approximately February 2014, some of the items were kept in the garage and the garage was not always locked. (CX0713-A (Gardner, Dep. at 45)). When Ms. Parr went to Mr. Daugherty's home to help finish up some network work there, Mr. Daugherty was not there and the garage door was up. (CX0713-A (Gardner, Dep. at 45-46)).

69. LabMD's retention of this Personal Information, continued operation of a computer network, and observed physical security issues demonstrates that "'there exists some cognizable danger of recurrent violation." *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (quoting *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)); *see also FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1087-88 (C.D. Cal. 2012) (finding permanent injunction appropriate where defendant continued to work in same business field, even though no longer involved in the same type of conduct); *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1337 (M.D. Fla. 2010) (finding that defendant's new business venture in a similar industry "presented significant opportunities for similar violations"); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393-94 (D. Conn. 2009) (imposing a permanent injunction where discontinued conduct was "obvious and

widespread" rather than "a single instance"). Furthermore, "[a] 'court's power to grant injunctive relief survives the discontinuance of the illegal conduct.'" *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (quoting *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)).

70. Injunctions issue based on the "'necessities of the public interest,'" balancing the interests of the parties who might be affected by the decision. *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (quoting *US v. Oakland Cannabis Buyers' Coop*., 532 U.S. 483, 496 (2001). Here, the interests to be balanced are the consumers' whose Personal Information LabMD holds, including consumers for whom LabMD performed no medical testing or other services, and LabMD's interests. As demonstrated *supra*, *see generally* § 9 (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) *et seq.* (¶¶ 1472-1798), future failures to maintain reasonable data security would likely result in substantial harm to consumers. *See FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009) (imposing injunction where "[f]uture violations of a similar nature would surely result in financial harm to consumers").

71. That LabMD is not currently collecting new specimens for testing is not a bar to entry of the notice order. *Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *92 (1984) (case not moot even where "the specific facts alleged" are "unlikely to arise again" if there is a possibility the respondent may "return to the general course of conduct with which it is charged").

72. Intentionally left blank.

1.4.2.1 An Injunction is an Appropriate Remedy

73. Factors to consider in determining whether to impose an injunction based on past conduct include: "the egregiousness of the defendant's actions, the isolated or recurrent nature of the infraction, the degree of scienter involved, the sincerity of the defendant's assurances against future violations, the defendant's recognition of the wrongful nature of his conduct, and the likelihood that the defendant's occupation will present opportunities for future violations." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) (quoting *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1017 (N.D. Ind. 2000). On the whole, these factors favor an injunction in this matter.

74. LabMD's data security failures were pervasive and persistent, rather than isolated, involving multiple types of problems over many years. *See, e.g., supra* CCFF §§ 5.2 (LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq.* (¶¶ 397-480) (many practices not memorialized until 2010, and 2010 written policies not comprehensive); 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) (for years and over multiple antivirus programs, LabMD did not consistently update virus definitions in its antivirus software,

run antivirus scans, or review the results of antivirus scans; and did not conduct penetration testing until 2010); 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) (never deleted any Personal Information, did not implement access controls over a long period of time); 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq.* (¶¶ 852-900) (failed to provide security training to IT and non-IT employees over many years); 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993) (employees used weak passwords for years, and LabMD did not centrally manage passwords or provide for effective enforcement of its password policies until 2010); 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043) (used operating systems and programs years after the vendors stopped supporting them, and failed to patch vulnerabilities years after vendors warned of risks); 5.8 (LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information) *et seq.* (¶¶ 1045-1110) (gave some employees administrative rights over their computers and unlimited internet access for years, stored backups of personal information on employee workstations for years).

75. LabMD, through its employees and contractors, made decisions regarding data security, such as failing to enforce its security policies, *supra* CCFF § 5.2.4 (LabMD Did Not Enforce Some of the Policies in its Policy Manuals) *et seq.* (¶¶ 458-480), failing to consistently run and review antivirus scans, *supra* CCFF § 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), haphazardly deploying incomplete and ineffective manual inspections, *supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 660-696), and permitting users on its system to use weak passwords for years, *supra* CCFF § 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993).

76. LabMD's failure to take responsibility for its lax data security and refusal to acknowledge its data security issues demonstrate the need for injunctive relief. *Compare, e.g.*, LabMD's Motion to Admit RX-543 – RX-548 at 6 (asserting that Complaint Counsel should have investigated Tiversa rather than LabMD in connection with the release of the 1718 File) *with* JX0001-A (Joint Stips. of Law and Fact) at 4 (stipulating that LimeWire was installed on the billing manager's computer and that 900 files, including the 1718 File, were designated for sharing).

77. "[T]he FTC need not show that the defendants are likely to engage in violations involving precisely the same conduct. An injunction is justified if the FTC shows that similar violations are likely to occur." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) (citing *TRW, Inc. v. FTC*, 647 F.2d 942, 954 (9th Cir. 1981); *see also FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007) (citing *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 632 (1953) ("[T]he Commission need not show that the defendants are likely to engage in the *same precise conduct* found to be in violation of the law, but rather only that similar violations are likely to occur." (emphasis original)); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393 (D. Conn. 2009)

("Injunctive relief looks to future harm and is designed to deter conduct rather than punish." (citation omitted)).

78. LabMD retains the Personal Information of 750,000 consumers, which continues to be at risk. (CX0766 (LabMD's Resps. and Objections to Reqs. for Admission) at 5, Adm. 23).

79. Intentionally left blank.

1.4.3 Fencing-In Relief is Appropriate

80. The seriousness and deliberateness of LabMD's data security failures, the duration of its unreasonable security practices, and the transferability of the risks posed by unreasonable data security to all 750,000 consumers on whom LabMD holds Personal Information warrant broad fencing-in relief. *See infra* CCCL ¶¶ 81-89; *infra* CCCL §§ 1.4.3.1 (LabMD's Failure to Address its Data Security Failures Was Deliberate) (¶¶ 91-103), 1.4.3.2 (LabMD's Data Security Failures Were Serious) (¶¶ 105-110), 1.4.3.3 (LabMD's Data Security Failures Are Transferrable) (¶¶ 112-114).

81. "[T]he Commission has wide discretion in its choice of a remedy deemed adequate to cope with the unlawful practices disclosed," and "is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952).

82. The Commission is permitted "to frame its order broadly enough to prevent respondents from engaging in similarly illegal practices in [the] future." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

83. The Commission can issue orders with fencing-in provisions that are broader than respondent's unlawful conduct. *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006).

84. Fencing-in provisions are appropriate where they are "reasonably related" to the conduct at issue. *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 216 (D. Mass. 2009). The fencing-in provisions in the Notice Order are related to Respondent's security practices and the protection of consumer Personal Information.

85. Fencing-in relief is appropriate to ensure that a respondent does not engage in similar practices in the future. *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citations omitted); *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1335 (M.D. Fla. 2010).

86. Factors to consider in determining whether fencing-in relief is appropriate include: "(1) the deliberateness and seriousness of the violation, (2) the degree of transferability of the violation to other products, and (3) any history of prior violations." *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citations omitted); *see also Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6 at *414-415 (1984).

87. "'The reasonable relationship analysis operates on a sliding scale – any one factor's importance varies depending on the extent to which the others are found. . . . All three

factors need not be present for a reasonable relationship to exist.'" *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 309 (May 17, 2012) (quoting *Telebrands Corp. v. FTC*, 457 F.3d 354, 358-59 (4th Cir. 2006)).

88. "[I]t is the circumstances of the violation as a whole, and not merely the presence of absence of any one [] factor, that justifies a broad order." *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (citations omitted).

89. "The more egregious the facts with respect to a particular element, the less important it is that another negative factor be present." *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 392 (9th Cir. 1982).

90. Intentionally left blank.

1.4.3.1 LabMD's Failure to Address its Data Security Failures Was Deliberate

91. LabMD, through its employees and contractors, had control over and made decisions regarding data security. (CX0709 (Daugherty, Dep. at 13-14) (testifying that other than the physical medical operations of LabMD, Mr. Daugherty had final authority over LabMD's operations); (CX0725-A (Martin, Dep. at 159), CX0727-A (Parr, Dep. at 105-06), CX0705-A (Bradley, Dep. at 136-37) (all stating that all IT expenditures at LabMD had to be approved by Mr. Daugherty); CX0724 (Maire, Dep. at 12) (testifying that Mr. Boyle directed the day-to-day work in the IT department at LabMD); (CX0733 (Boyle, LabMD Designee, IHT) at 60-61) (confirming that Mr. Boyle and Mr. Daugherty were the final approvers for any IT security policies); (CX0733 (Boyle, LabMD Designee, IHT) at 92-93, 104, 125-26, 147, 202, 204) (explaining that LabMD's memorialized security policies in 2010 were written by Mr. Boyle, Mr. Hyer, Mr. Daugherty, and Ms. Gilbreth and approved by Mr. Boyle and Mr. Daugherty)).

92. Even where LabMD had policies for data security in place, it often violated or failed to fully implement the policies. *See infra* CCCL ¶¶ 93-103.

93. For example, LabMD's policies as memorialized in 2010 required employees to encrypt emails containing sensitive information. However, LabMD did not provide employees with tools with which to encrypt email containing sensitive information. *See supra* CCFF § 5.2.4.3 (LabMD Did Not Enforce Its Recommendation That Employees Encrypt Emails (¶¶ 474-480)).

94. Another of LabMD's policies memorialized in 2010 required the identification and removal of unauthorized software; however, for as long as three years an employee with access to Personal Information had installed and used an unauthorized P2P file-sharing program. *See supra* CCFF §§ 5.2.4.1 (LabMD Did Not Enforce Its Policy to Restrict Downloads from the Internet (¶¶ 458-462), 5.2.4.2 (LabMD Did Not Enforce Its Policy To Detect and Remove Unauthorized Applications) (¶¶ 465-471)).

95. LabMD adopted a compliance program in January 2003 which required the company to implement policies and procedures to "monitor and insure that patient information is

secure, kept private and only used for care, billing or operational uses." (CX0005 (LabMD Compliance Program effective Jan. 2003) at 4). However, LabMD did not implement any policies or procedures to satisfy these information security requirements, and did not create written policies until 2010. *See supra* CCFF § 5.2.2.1.2 (LabMD's Compliance Program Was Not a Comprehensive Written Information Security Program) (¶¶ 434-438).

96. LabMD's employees and outside contractors notified LabMD that its security was inadequate, and LabMD failed to act on those warnings within a reasonable time frame. *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (finding a violation deliberate where the company did not act on warnings); *see infra* CCCL ¶¶ 97, 102-103. LabMD's conduct shows a pattern of carelessness and delay, and demonstrates the deliberateness of its data security failures.

97. LabMD had notice of a security breach relating to P2P file sharing as early as May 2008. *See supra* CCFF § 8.1.3 (1718 File Found on Peer-to-Peer Network) (¶ 1395).

98. LabMD had a policy prohibiting employees from using the Internet for non-work purposes; this would include downloading software and the use of peer-to-peer file-sharing. (CX0001 (LabMD Employee Handbook Rev. June 2004) at 7; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 7; CX0714-A ([Fmr. LabMD Empl.], Dep. at 38); CX0730 (Simmons, Dep. at 16-17, 93); RX0481 (LabMD Electronics Policy (2004) (prohibits personal Internet use).

99. However, even after May 2008, LabMD did not provide non-IT employees with any training regarding security mechanisms or the consequences of reconfiguring security settings in applications. *See supra* CCFF § 5.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information) *et seq.* (¶¶ 866-891).

100. Furthermore, many LabMD employees were given administrative rights over their workstations, which allows a user to download software, such as peer-to-peer file-sharing software. *See supra* CCFF § 5.8.1 (LabMD Employees Were Given Administrative Access to Workstation Computers) (¶¶ 1056-1063).

101. LabMD's manual computer inspections were not proactively deployed to search out unauthorized uses of LabMD's network, but were used only in response to employee issues with their workstations. *See supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) *et seq.* (¶¶ 660-696). Furthermore, manual inspections are not an adequate substitute for automated mechanisms. *See supra* CCFF § 5.3.2.3 (LabMD's Manual Inspections Could Not Reliably Detect Security Risks) (¶¶ 660-665).

102. When a third party identified security issues on LabMD's servers and provided solutions, LabMD failed to remediate the problems over several months. (*Supra* CCFF §§ 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)(vulnerability identified in May 2010 scan still present in July 2010); 5.3.4.3.1.3 (The Mapper Server Had a Vulnerability

that Could Be Exploited To Access Any Files Available On Mapper) (¶¶ 781-788) (vulnerability identified in May 2010 scan still present in July 2010); 5.3.4.3.1.4 (The Mapper Server Had a Vulnerability that Could Be Exploited To Steal FTP Usernames and Passwords) (¶¶ 792-797) (vulnerability identified in May 2010 scan still present in September 2010)).

103. LabMD also failed to update its antivirus software for several months even after it was informed that the software was no longer supported. *Supra* CCFF § 5.3.2.1.1.1 (LabMD Did Not Consistently Update Symantec Virus Definitions on Servers) (¶¶ 547-550).

104. Intentionally left blank.

1.4.3.2 LabMD's Data Security Failures Were Serious

105. LabMD's data security failures were serious: LabMD failed to provide reasonable security for Personal Information within its computer network. (CX0740 (Hill Report) ¶ 49)); *see also supra* CCFF § 5 (LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Network) *et seq.* (¶¶ 382-1110).

106. The seriousness of the violations in this case are illustrated by the types of Personal Information LabMD holds, *supra* CCFF § 9.2.1 (LabMD Stores the Types of Information Used to Commit Identity Frauds) (¶¶ 1642-1643), and the harm likely to be caused to consumers, including identity theft, medical identity theft, and other harms, by breach of this Personal Information. *Supra* CCFF § 9.2 (LabMD's Security Failures Placed All Consumers Whose Personal Information is on Their Network at Risk) *et seq.* (¶¶ 1642-1658).

107. The seriousness of the violations are also illustrated by the duration of LabMD's data security failures. *See Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (finding a violation serious due to, inter alia, its two and one-half year duration); *see, e.g., supra* CCCL § 1.4.2.1 (An Injunction is an Appropriate Remedy) (¶¶ 73-78).

108. The inability of consumers to protect themselves from the risks LabMD's failures posed to their Personal Information is another indicium of seriousness. *See Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 312 (May 17, 2012) (finding violation serious where consumers did not have to ability to evaluate health claims made in advertisement); *Thompson Med. Co*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6 at *414-17 (finding violation serious where consumers could not readily judge the truth or falsity of the claims at issue); *supra* § 9.5.1 (The Consumer Is Not in a Position to Know of a Company's Security Practices) *et seq.* (¶¶ 1773-1795).

109. The seriousness of the violations in this case are illustrated by the breaches of the 1718 File and the Day Sheets. *Supra* CCFF § 8 (Security Incidents at LabMD) *et seq.* (¶¶ 1354-1469).

110. Complaint Counsel alleged a number of data security failures in its Complaint. (Compl. ¶ 10). Even if LabMD is not found to have maintained unfairly unreasonable security as to each of the items, its failures are still serious and warrant fencing-in relief. *Cf. Bristol-*

Myers Co., 102 F.T.C. 21, 1983 FTC LEXIS 64 at *377-80 (1983); *Fedders Corp.*, 85 F.T.C. 38, 1975 FTC LEXIS 282, at *71-72 (1975) (both finding fencing-in relief appropriate even where only a small number of products or advertisements were found to violate Section 5).

111. Intentionally left blank.

1.4.3.3 LabMD's Data Security Failures Are Transferable

112. "The prevention of 'transfers' of unfair trade practices is a fundamental goal of the Commission's remedial work." *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 394 (9th Cir. 1982).

113. LabMD's data security failures continue to place the Personal Information of all 750,000 consumers in its possession at risk, not just those included in the 1718 File and Day Sheets. Furthermore, if LabMD resumes collecting the Personal Information of additional consumers, its failures place those consumers at risk as well. Because LabMD retains the Personal Information of 750,000 consumers, has not dissolved as a Georgia corporation, and does not intend to dissolve or to safely dispose of consumers' Personal Information, the dangers posed by LabMD's conduct are transferable to any future forms of operation the company might take. *See FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 215 (D. Mass. 2009) (imposing fencing-in injunction "[e]ven though the [] defendants currently have no employees and are not engaged in any business, they could resume such activities in the future"); *U.S. v. Bldg. Insp. of Am.*, 894 F. Supp. 507, 521 (D. Mass. 1995) (finding injunction appropriate where company had ceased operation but "remains a going concern and could resume at any time"); *cf. Int'l Harvester Co.*, 104 FTC 949, 1984 WL 565290 at *92 (1984) ("[A]n obligation should ordinarily extend as long as the risk of harm exists.").

114. There are no steps that consumers can take themselves to protect their Personal Information that LabMD currently holds and prevent future harm. *Supra* CCFF § 9.2.2 (LabMD's Failure to Secure the Personal Information it Stores Places Consumers at Greater Risk of Identity Theft) (¶¶ 1653-1658). Consumers did not know, in most cases, that their Personal Information was sent to LabMD nor its security practices, *supra* CCFF § 9.5.1 (The Consumer Is Not in a Position to Know of a Company's Security Practices) *et seq.* (¶¶ 1773-7797), CCCL § 1.3.2 (Consumers Cannot Reasonably Avoid the Substantial Injury Caused or Likely to Be Caused by LabMD's Data Security Failures) (¶¶ 42-44), and even if they did have such knowledge identity theft cannot be fully remediated after notice, *supra* CCFF § 9.4.2.5.1. (Consumers Cannot Avoid All Harms Through Notification of Unauthorized Disclosures of Information) (¶¶ 1769-1770).

115. Intentionally left blank.

1.4.3.4 The History of LabMD's Data Security Failures Warrants Fencing-In Relief

116. There is no evidence of prior violations of the FTC Act by LabMD. Where the first two factors sufficiently establish a reasonable relationship between the remedy and the

violation, this factor is not necessary to the appropriateness of fencing-in relief in an order. *Telebrands Corp. v. FTC*, 457 F.3d 354, 362 (4th Cir. 2006); *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012).

117. However, LabMD's conduct occurred over a long period of time, which indicates both seriousness and continuous violations. LabMD's data security failures persisted from at least 2005 through at least the close of evidence in the hearing. *See, e.g.*, *supra* CCFF §§ 5.2.2 (Before 2010 LabMD Did Not Have Written Information Security Policies) *et seq.* (¶¶ 415-443); 5.3.4 (LabMD Did Not Use Penetration Testing Before 2010) (¶¶ 715-726); 5.4.2.1 (LabMD Had No Policy for Deleting Personal Information and Maintained the Information Indefinitely) (¶¶ 835-841) (LabMD has retained all the Personal Information it has ever collected); 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) *et seq.* (¶¶ 852-900) (LabMD did not provide employees any training on data security); 5.6.2.2 (LabMD Did Not Prevent Employees from Using the Same Password for Years) (¶¶ 954-957) (employee used insecure login credentials from 2006 through 2013); 5.7.1 (Some LabMD Servers Used a Windows Operating System Years After Microsoft Had Stopped Updating and Supporting It) (¶¶ 1003-1008).

118. LabMD's data security failures were diverse, and covered a wide spectrum of data security practices, including failure to develop, implement, and maintain a comprehensive information security program, *supra* CCFF § 5.2 (LabMD Did Not Develop and Maintain a Comprehensive Written Information Security Program) *et seq.* (¶¶ 397-480); failure to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network, *supra* CCFF 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); failure to use adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs, *supra* CCFF § 5.4 (LabMD Did Not use Adequate Measures to Prevent Employees From Accessing Personal Information Not Needed to Do Their Jobs) *et seq.* (¶¶ 811-849); failure to train employees to safeguard Personal Information, *supra* 5.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information) (*et seq.* (¶¶ 852-900); failure to require employees or other users with remote access to the networks to use authentication-related security measures, *supra* CCFF § 5.6 (LabMD Did Not Require Common Authentication-Related Security Measures) *et seq.* (¶¶ 903-993); failure to maintain and update operating systems of computers and other devices on its network, *supra* CCFF § 5.7 (LabMD Did Not Maintain and Update Operating Systems and Other Devices) *et seq.* (¶¶ 996-1043); and failure to use readily available measures to prevent or detect unauthorized access to Personal Information on its computer networks, *supra* CCFF § 5.8 (LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information) *et seq.* (¶¶ 1045-1110).

119. These facts demonstrate a history of violations of the unfairness provision of the FTC Act.

120. The lack of prior adjudicated violations of the FTC Act is not a bar to entry of fencing-in provisions. *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (concluding claim that

fencing-in provision was inappropriate because of a lack of prior violations "without merit").

121. Intentionally left blank.

1.4.4 The Notice Order's Provisions are Appropriate

1.4.4.1 The Twenty Year Duration of the Order is Appropriate

122. A twenty year order duration is consistent with the Commission's prior orders. *See, e.g.*, *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012); *Daniel Chapter One*, Docket No. 9329, 2010 FTC LEXIS 11, at *9-10.

123. A twenty year order duration is appropriate given the length of time over which LabMD's unreasonable data security practices extended. *Supra* CCCL ¶ 117; *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012) (finding 20 year order duration appropriate where advertisements were disseminated over a course of at least 6 years).

124. Intentionally left blank.

1.4.4.2 Part I: Comprehensive Information Security Program

125. Part I of the Notice Order requires LabMD to establish, implement, and maintain a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of Personal Information collected from or about consumers. The program must be in writing, and should contain administrative, technical, and physical safeguards appropriate to LabMD's size and complexity, the nature and scope of its activities, and the sensitivity of the Personal Information collected from or about consumers. The safeguards must include (A) the designation of an employee or employees to coordinate and be accountable for the information security program; (B) the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks; (C) the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures; (D) the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and (E) the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

126. Part I's requirement for the establishment, implementation, and maintenance of a comprehensive information security program is reasonably related to, and highly

correlated with, the allegations of the Complaint, which alleges in Paragraph 10(a) that LabMD "did not develop, implement, or maintain a comprehensive information security program to protect consumers' Personal Information." Compl. ¶ 10(a).

127. Part I of the Notice Order is consistent with the provisions in the Commission's Safeguards Rule of the Gramm-Leach Bliley Act. 16 C.F.R. § 314.4.

128. Part I of the Notice Order is also consistent with relief approved in Commission settlements relating to unfair data security practices. *See, e.g.*, CCCL ¶¶ 17, 18; *see also U.S. v. Consumer Portfolio Servs., Inc.*, Case No. 8:14-cv-00819-ABC-RNB, at 6-7, Section IV (Stipulated Order for Perm. Injunct.) (C.D. Cal. June 11, 2014), available at http://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc (requiring debt collector to implement a comprehensive data integrity program with elements similar to a comprehensive data security program).

129. The Commission has provided a large amount of guidance to businesses for complying with the Safeguards Rule and on general data security practices. *See, e.g.*, Financial Institutions and Customer Information: Complying with the Safeguards Rule, *available at* http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule; Protecting Personal Information: A Guide for Business, *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; *see generally* FTC Bureau of Consumer Protection Business Center: Data Security, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

130. Other sources, such as NIST, SANS, and US CERT, have also provided guidance for implementing a comprehensive information security program. (*Supra* CCFF § 6.2 (Comprehensive Information Security Program) (¶¶ 1121-1124)).

131. Given this extensive guidance, the provision is sufficiently clear and precise that its requirements can be understood, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965) (citing *FTC v. Henry Broch & Co.*, 368 U.S. 360, 367-68 (1962)).

132. Intentionally left blank.

1.4.4.3 Part II: Initial and Biennial Assessments

133. Part II of the Notice Order requires LabMD to obtain initial and then biennial assessments and reports for twenty years from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The Notice Order provides examples of the types of qualifications that are sufficient for such qualified, objective, and independent third-party professionals.

134. The provision enumerates the elements that must be included in the assessment, which must: (1) set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained; (2) explain how the safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Personal Information collected from or about

consumers; (3) explain how the safeguards that have been implemented meet or exceed the provisions in Part I of the order; and (4) certify that respondent's security program provides reasonable assurance that the security, confidentiality, and integrity of Personal Information is protected.

135. This provision is consistent with prior Commission orders in data security cases. *See, e.g.*, Conclusions of Law ¶¶ 17, 18.

136. Such independent third-party review is appropriate fencing-in relief. *See Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/05/120521pomdecision.pdf (the requirement of competent and reliable scientific evidence "based on the expertise of professionals in the relevant area" is "typical"); *see, e.g., U.S. v. Consumer Portfolio Servs., Inc.*, No. 8:14-cv-00819-ABC-RNB, Section V at 8-9 (Stip. Order for Perm. Injunct.) (C.D. Cal. June 11, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc (requiring that defendant obtain an assessment and report regarding its comprehensive data integrity program from a qualified, objective, independent, third-party professional); *FTC v. Smolev*, No. 01-8922 CIV-Zloch Sections V.B.2 at 17, VI at 18-20 (Stip. Final Judgment) (S.D. Fla. Oct. 24, 2001), *available at* http://www.ftc.gov/enforcement/cases-proceedings/992-3255/smolev-ira-bruce-turiansky-triad-discount-buying-service-inc (requiring, under certain circumstances, defendant to use an independent third-party verifier for telemarketing transactions); *FTC v. Special Data Processing Corp.*, Case No. 8:04-cv-1955-T-23EAJ, Sections IV.B.3. at 13 and V. at 13-15 (Stip. Judgment) (M.D. Fla. Sept. 30, 2004), *available at* http://www.ftc.gov/enforcement/cases-proceedings/002-3213/special-data-processing-corporation (Stip. Judgment) (M.D. Fla. Sept. 29, 2004) (requiring, under certain circumstances, defendant to use an independent third-party verifier for telemarketing transactions); *cf. Removatron Int'l Corp.*, 111 F.T.C. 206, 305-06 (1988) (according "substantial weight" to FDA determination regarding product).

137. Intentionally left blank.

1.4.4.3.1 Part II's Fencing-In Provision is Appropriate

138. Fencing-in relief is "designed to prevent future unlawful conduct, and provides for order provisions that are broader than the conduct found to violate Section 5." *Telebrands Corp. v. FTC*, 457 F.3d 354, 357 n.5 (4th Cir. 2006) (citing *Telebrands*, 140 F.T.C. 278, 281 n.3 (2005)); *Am. Home Prods. v. FTC*, 695 F.2d 681, 705 (3d Cir. 1982); *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citing *FTC v. Colgate-Palmolive*, 380 U.S. 374, 395 (1965)); *Sears v. FTC*, 676 F.2d 385, 391-92 (9th Cir. 1982)).

139. The Commission's "wide discretion" to craft that remedy is subject to only two constraints: the order must bear a "reasonable relation" to the unlawful practices, *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946); and it must be sufficiently clear and precise that its requirements can be understood, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965).

140. Pursuant to this discretion, courts have affirmed Commission orders requiring remedies as diverse as prohibitions on individual use of zone pricing (*FTC v. Nat'l Lead Co*., 352 U.S. 419, 431 (1957)); cancellation of existing contracts (*North Tex. Specialty Physicians v. FTC*, 528 F.3d 346, 372 (5th Cir. 2008)); mandated divestiture of assets to create a competitor (*Chicago Bridge & Iron Co. N.V. v. FTC*, 534 F.3d 410, 441 (5th Cir. 2008)); requirements for varying levels of substantiation for future claims (*See, e.g*., *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 389 n.10, 400 (9th Cir. 1982) (requiring competent and reliable evidence for future performance claims for major household appliances); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192, 197 (D.C. Cir. 1986) (requiring at least two adequate and well-controlled, double-blinded clinical studies for future efficacy claims for a topical analgesic)); disclosure requirements (*Porter & Dietsch, Inc. v. FTC*, 605 F.2d 294, 306-07 (7th Cir. 1979)) and trade name excision (*Cont'l Wax Co. v. FTC*, 330 F.2d 475, 479-80 (2d Cir. 1964)). The underlying inquiry in all these orders is the same: what is the necessary remedy to ensure that respondents do not again violate the FTC Act? *See FTC v. Colgate-Palmolive Co*., 380 U.S. 374, 392 (1965).

141. The Commission may order "provisions that are broader than the conduct that is declared unlawful." *Telebrands Corp*., 457 F.3d at 357 n.5 (citing *Telebrands*, 140 F.T.C. at 281 n.3); *see also, e.g*., *FTC v. Colgate-Palmolive Co*., 380 U.S. 374, 394-95 (1965); *FTC v. Ruberoid Co*., 343 U.S. 470, 473 (1952); *POM Wonderful*, 2013 FTC LEXIS 6, at *50 (Jan. 10, 2013), *aff'd* 777 F.3d 478 (D.C. Cir. 2015). To the extent the proposed notice order goes beyond LabMD's specific practices, such fencing-in relief is appropriate in light of LabMD's multiple and systemic data security failures. The Notice Order is narrowly crafted to prevent LabMD from continuing to place consumers' Personal Information at risk, while still allowing LabMD to collect, use, and store Personal Information to conduct its business.

142. This fencing-in relief is reasonably related to LabMD's conduct. *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612 (1946). Even where the company had data security policies, it did not adequately enforce them, or provide the tools needed to implement them. *Supra* CCFF § 5.2.4 (LabMD Did Not Enforce Some of the Policies in its Policy Manuals) *et seq.* (¶¶ 458-480). For example, despite a policy against the installation of installation of personal programs and personal use of the Internet, LimeWire was installed and used a LabMD employee's computer. *See supra* CCFF §§ 5.2.4.1 (LabMD Did Not Enforce Its Policy to Restrict Downloads from the Internet) (¶¶ 458-462), 8.1.2 (1718 File Shared on Gnutella Network through LimeWire on a LabMD Billing Computer) (¶¶ 1363-1372), CCCL § 1.4.3.1 (LabMD's Failure to Address its Data Security Failures was Deliberate) (¶¶ 91-103). Although LabMD's policies stated that emails containing sensitive information were required to be encrypted, employees testified that no tools were provided to encrypt such emails. *See supra* CCFF § 5.2.4.3 (LabMD Did Not Enforce Its Recommendation that Employees Encrypt Emails) (¶¶ 474-480).

143. A fencing-in provision must be "sufficiently clear that it is comprehensible to the violator, and must be 'reasonably relat[ed]' to a violation of the act." *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (citing *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965)).

144. The four provisions of the fencing-in relief laid out in Part II, along with the necessary credentials of the third party, are clear and precise, particularly given that a virtually identical provision has been imposed in many of the Commission's past orders. (*Supra* CCCL ¶ 18).

145. Intentionally left blank.

1.4.4.4 Part III: Notice to Affected Individuals

146. Part III of the Notice Order requires LabMD to notify Affected Individuals in the 1718 File regarding the unauthorized disclosure of their Personal Information.

147. Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information or that they can take actions to reduce their risk of harm from identity crime. (*Supra* CCFF § 9.3.4.3 (With No Notification of Unauthorized Disclosure, No Mitigation of Harm is Possible) (¶¶ 1708-1711).

148. Notice to affected consumers is an appropriate remedy. *Int'l Harvester Co.*, 104 FTC 949, 1009 (1984) (noting that an order requiring disclosure of a hazard to consumers "is our ordinary and presumptive response" that is appropriate "even when the respondent has ceased engaging in the conduct in question"); *see also FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007) (noting, where defendant's had unfairly procured the consumers' phone records, that consumer notice may be an appropriate equitable remedy) and No. 2:06-CV-105-WFD (Order and Judgment for Permanent Injunction and Other Equitable Relief) (Dec. 20, 2007) (requiring defendant to provide FTC with contact information for affected consumers so the Commission could provide notice); *FTC v. Bayview Solutions, LLC,* Case No. 1:14-cv-01830, at 7, Section IV (Stip. Prelim. Injunct.) (D.D.C. Nov. 3, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/150421bayviewstip.pdf (requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *FTC v. Cornerstone & Co., LLC,* Case No. 1:14-CV-01479, Section IV at 7 (Prelim. Injunct.) (D.D.C. Sept. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141001cornerstoneorder.pdf (requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *U.S. v. InfoTrack Info. Svcs, Inc*., No. 1:14-cv-02054 (N.D. Ill. Mar. 25, 2014) (Stip. Final Judgment), *available at* https://www.ftc.gov/system/files/documents/cases/140409infotrackorder_0.pdf (requiring notice to consumer that was included in a sex offender registry consumer report when information provided to potential employers); *TRENDnet, Inc.*, FTC Docket No. C-4426, FTC File No. 122-3090 (FTC Sept. 4, 2013) (consent order), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf (notice of security flaw that may have allowed unauthorized users to view live feed of in-home cameras); *Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (FTC Feb.

20, 2013) (consent order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competedo.pdf (notice that personal information may have been transmitted insecurely); *Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (FTC Mar. 27, 2012) (consent order), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf (notice that personal information may have been transmitted insecurely).

149. Notice to Affected Consumers' insurance companies is also an appropriate remedy, to provide them with an opportunity to protect consumers' identity from misuse. Third party notices are a commonly used remedy to mitigate harms. *See, e.g., PPG Architectural Finishes, Inc*., No. C-4385, 2013 FTC LEXIS 22, at *8-9, 13-14 (Mar. 5, 2013) (consent order) (notices sent to dealers, distributors, and other entities to stop using prior advertising materials with deceptive no VOCs claim for paint and to apply the enclosed stickers to product labeling); *Oreck Corp*., 151 F.T.C. 289, 371-72, 376-77 (May 19, 2011) (consent order) (notice sent to franchisees); *Indoor Tanning Ass'n*., 149 F.T.C. 1406, 1439, 1443-44 (May 13, 2010) (notices sent to association members and other prior recipients of point-of-sale materials); *Cytodyne LLC,* 140 F.T.C. 191, 209, 214-15 (Aug. 23, 2005) (consent order) (notices sent to purchaser for resale of weight-loss supplement); *Snore Formula, Inc*., 136 F.T.C. 214, 298-99, 304-05 (July 24, 2003) (consent order) (notices sent to distributors who had purchased the product from the respondents or one of the respondents' other distributors); *MaxCell BioScience, Inc*., 132 F.T.C. 1, 58-59, 66-67 (July 30, 2001) (consent order) (notice to distributors); *Alternative Cigarettes, Inc*., No. C-3956, 2000 FTC LEXIS 59, at *24, 31-33 (Apr. 27, 2000) (consent order) (notices to retailers, distributors, or other purchasers for resale to which respondents supplied cigarettes); *Body Sys. Tech., Inc*., 128 F.T.C. 299, 312, 318-19 (Sept. 7, 1999) (consent order) (notice to distributors); *Brake Guard Prods., Inc*., 125 F.T.C. 138, 259-60, 263-64 (Jan. 15, 1998) (consent order) (notice to resellers); *Phaseout of Am., Inc*., 123 F.T.C. 395, 457, 461-63 (Feb. 12, 1997) (consent order) (notice to resellers); *Consumer Direct, Inc*., No. 9236, 1990 FTC LEXIS 260, at *10-11, 20-21 (May 1, 1990) (consent order) (notice to credit card syndicators); *Third Option Labs., Inc*., 120 F.T.C. 973, 996, 1001 (Nov. 29, 1995) (consent order) (notice to resellers); *Canandaigua Wine Co*., 114 F.T.C. 349, 359-60 (June 26, 1991) (consent order) (notice to distributors and retailers).

150. Equitable relief, including for consumer notice, "remain[s] viable even if an injunction is otherwise unnecessary." *FTC v Accusearch, Inc.*, 2007 WL 4356786 at *9 (D. Wyo. Sept. 28, 2007).

151. LabMD has provided notice to consumers in the Day Sheets, *supra* CCFF § 8.2.4.1 (LabMD Notice to Affected Consumers) (¶¶ 1461-1469), indicating that this Order provision is reasonable. *Daniel Chapter One*, Docket No. 9329, 2009 FTC LEXIS 157, at *275 (noting that the Commission has "considerable discretion in fashioning an appropriate remedial order").

152. Intentionally left blank.

1.4.4.5 Parts IV-VIII: Recordkeeping Provisions

153. One of the purposes of injunctive relief is "monitoring compliance with the law and the terms of the injunction." *FTC v. Direct Mkting. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009).

154. Monitoring provisions to ensure compliance with injunctions are appropriate to include in FTC orders. *FTC v. RCA Credit Svcs, LLC*, 727 F. Supp. 2d 1320, 1335 (M.D. Fla. 2010).

155. The recordkeeping provisions in Parts IV-VIII of the Notice Order are consistent with those in other FTC orders. *See, e.g.*, cases cited in CCCL ¶ 19; *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012). Part IV is a record-keeping requirement. Part V sets forth Order distribution requirements. Part VI requires LabMD to file notifications about changes in corporate structure. Part VII sets forth compliance reporting requirements. Finally, Part VIII is a sunsetting provision.

156. Intentionally left blank.

Dated: August 10, 2015

Respectfully submitted,

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Ryan Mehm
Jarad Brown
Federal Trade Commission
600 Pennsylvania Ave., NW
Room CC-8232
Washington, DC 20580
Telephone: (202) 326-2999
Facsimile: (202) 326-3062
Electronic mail: lvandruff@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on August 10, 2015, I caused the foregoing document to be filed electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

I also certify that I caused to be delivered by hand an electronic copy and four hard copies of the foregoing document to:

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

I further certify that I caused a copy of the foregoing document to be served *via* secure file transfer to:

Daniel Epstein
Patrick Massari
Prashant K. Khetan
Erica Marshall
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
daniel.epstein@causeofaction.org
patrick.massari@causeofaction.org
prashant.khetan@causeofaction.org
erica.marshall@causeofaction.org

Reed Rubinstein
William A. Sherman, II
Sunni Harris
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com
william.sherman@dinsmore.com
sunni.harris@dinsmore.com
Counsel for Respondent LabMD, Inc.

CERTIFICATE FOR ELECTRONIC FILING

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

August 10, 2015 By: ________________

Jarad Brown
Federal Trade Commission
Bureau of Consumer Protection