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

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

COMPLAINT COUNSEL'S
PRE-TRIAL BRIEF

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown
Counsel Supporting the Complaint

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580

PUBLIC

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Cases

Administrative Materials

Other Authorities

I. INTRODUCTION

Respondent LabMD, Inc. ("LabMD") engaged in fundamental, systemic security failures that put at risk consumers' sensitive personal and health information. As a result of LabMD's failures—which continued unabated for years—a file containing the sensitive Personal Information of approximately 9,300 consumers was shared to a public file sharing network without being detected by LabMD. The sensitive information included consumers' names, dates of birth, Social Security numbers, information relating to laboratory tests conducted, and health insurance policy numbers. These are exactly the kinds of personal data used to perpetrate identity theft. Indeed, LabMD documents containing consumers' sensitive Personal Information were also found in the possession of identity thieves in Sacramento, California. LabMD's failure to adopt reasonable and appropriate measures to protect consumers' sensitive Personal Information caused or is likely to cause substantial consumer injury that is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or competition. In this regard, LabMD violated Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

II. STATEMENT OF FACTS[1]

To aid the Court's review of the evidence, appended to this brief are a glossary of industry terms,[2] descriptions of the individuals who provided testimony or are otherwise related to this case,[3] and a timeline of IT employees' tenure at LabMD.[4]

A. Respondent

1. LabMD's Business

Respondent LabMD is a Georgia corporation. Its principal place of business was previously at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339 (Ans. ¶ 1; CX0766[5]), and since at least January 2014 is at 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339 (CX0766[6]) and [redacted] (CX0710, CX0709[7]). From at least 2001 through approximately December 2013 or January 2014, LabMD was in the business of conducting clinical laboratory tests on specimen samples from consumers

[1] Complaint Counsel's Pre-Trial Brief includes citations to exhibits Complaint Counsel intends to introduce at the evidentiary hearing. Where Complaint Counsel cites to the reports of its expert witnesses, Respondent's Answer, or legal authority, full citations are provided in the text. Where Complaint Counsel cites to other evidence, the CX reference is provided in the text and the pin citation is provided in the corresponding footnote with a parenthetical explanation.

[2] Exhibit 1.

[3] Exhibit 2.

[4] Exhibit 3.

[5] Ans. ¶ 1; CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 5.

[6] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 6; CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 10.

[7] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 193-94; CX0709 (Daugherty Dep. Tr.) at 22-23.

and reporting test results to physicians. Ans. ¶ 3; CX0765; CX0291.[8] Respondent has tested samples from states outside of Georgia, including Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona. Ans. ¶ 5; CX0766.[9] Starting in approximately December 2013 or January 2014, Respondent stopped accepting specimen samples and conducting tests; it still provides past test results to health care providers and continues to collect on monies owed to it. CX0291; CX0765.[10]

2. LabMD's Collection and Maintenance of Consumers' Personal Information

In connection with performing tests, LabMD has collected and continues to maintain consumers' Personal Information.[11] It files insurance claims for charges related to clinical laboratory tests with health insurance companies. Ans. ¶ 4. 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,

[8] Ans. ¶ 3; CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 10 (stating LabMD ceased accepting new specimens on Dec. 20, 2013); CX0291 (LabMD Letter to Physicians Offices re: Closing) (stating that LabMD will stop accepting new specimens Jan. 11, 2014).

[9] Ans. ¶ 5; CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admissions 7-11 (tested specimens of consumers and provided test results to physicians located in at least seven states).

[10] CX0291 (LabMD Letter to Physicians Offices re: Closing); CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 10.

[11] "Personal Information" means individually identifiable information from or about a consumer including: (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. CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) at 1.

addresses, and telephone numbers; laboratory tests, test codes, and diagnoses; clinical histories; and health insurance company names and policy numbers. Ans. ¶ 6, CX0766, CX0765.[12] In addition, Respondent received payment information directly from consumers. Insured patients may pay the part of Respondent's charges not covered by insurance, and uninsured patients may be responsible for the full amount of the charges. Ans. ¶ 4. Consumers pay LabMD's charges with credit cards, debit cards, or personal checks. CX0766; CX0706; CX0765.[13]

LabMD maintains Personal Information on over 750,000 consumers (CX0766[14]), including copies of hundreds of personal checks (*Id.*[15]). Among the data is Personal Information regarding approximately 100,000 consumers for whom LabMD never performed testing. CX0766; CX0710; CX0718; CX0726.[16] LabMD does not delete or destroy Personal Information

[12] Ans. ¶ 6 (names; addresses; dates of birth; gender; telephone numbers; Social Security numbers; referring health care provider names, addresses, and telephone numbers; laboratory tests and test codes; health insurance company names and policy numbers); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 25 (diagnoses and laboratory results); CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 13 (referencing CX0790 (Complaint Counsel's First Set of Interrogs. to Resp't) definition 9 "Personal Information" at 2) (*inter alia*, medical record numbers; bank routing, account, and check numbers; credit or debit card information, such as account number; clinical histories).

[13] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 29 (checks); CX0706 (Brown Dep. Tr.) at 39-40 (describing process for consumers to pay with credit cards); CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 13 (referencing CX0790 (Complaint Counsel's First Set of Interrogs. to Resp't) definition 9 "Personal Information" at 2) (LabMD possesses credit and debit card information of consumers).

[14] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers).

[15] *Id.* Admission 32.

[16] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers); CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 185-90, 192-94, 198-99 (LabMD performed no tests for 20-25% of consumers on whom it received and maintains personal information, and other labs performed tests on 20-25% of patients for whom LabMD did not perform tests). Based on these data, LabMD maintains the personal information of no fewer than 100,000 consumers for whom it performed no lab test. *See also* CX0718 (Hudson Dep. Tr.) at 23-24; 52-54, 59-62 (testifying that, beginning in January 2005, it was LabMD's practice to transfer every patient's information to the company, regardless of whether LabMD performed a test for the patient); CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 43-

of consumers, but maintains it indefinitely. CX0710.[17] LabMD currently maintains the Personal Information of consumers at 1250 Parkwood Circle, Unit 2201, Atlanta GA 30339, a condominium used as an office (CX0765[18]), and [redacted] the personal residence of LabMD's President and Chief Executive Officer, (CX0710, CX0709[19]).

B. LabMD's Computer Network

1. Network Devices and Configuration

LabMD's network consisted of: computers LabMD provided to physician clients to use from their offices to place orders, submit consumers' Personal Information to LabMD, and retrieve results over the Internet; and equipment located at LabMD's business premises, including computers used by employees, servers, hardware needed to allow connections among these devices and the Internet, and software of various types. CX0740 (Hill) ¶¶ 32, 35; CX0034; CX0039; CX0202; CX0711; CX0552; CX0734; CX0584; CX0735.[20] In January 2014, LabMD

45, 80 (testifying that the name, date of birth, address, Social Security number, billing and insurance information of all Southeast Urology Network patients was sent to LabMD, regardless of whether LabMD performed tests for the patients).

[17] CX0710 (Daugherty, Lab MD Designee, Dep. Tr.) at 60, 215-16, 220-21.

[18] CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 17.

[19] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 193-94; CX0709 (Daugherty Dep. Tr.) at 22-23.

[20] CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location); CX0039 (Network Diagram – Powers Ferry Road Location Apr. 2009); CX0202 (Network Diagram – Drawn by Jeremy Dooley at Deposition); CX0711 (Dooley Dep. Tr.) at 22-29; CX0552 (Network Diagram Hand-drawn at Simmons IH); CX0734 (Simmons Invest. Hrg. Tr). at 32-39; CX0584 (Network Diagram Hand-drawn at Kaloustian IH); CX0735 (Kaloustian Invest. Hrg. Tr.) at 48-61.

moved this network from its business premises. CX0705; CX0725; CX0727.[21] Part of the network was moved to the private residence of LabMD's owner (CX0725; CX0727[22]); the rest of the equipment was moved to a nearby condominium that he owns (CX0725; CX0727; CX0709[23]). Located at the private residence and networked together are servers, several workstation computers, printers, and an internet connection. CX0705; CX0725; CX0727.[24] Located at the condominium is a workstation that can remotely connect to a server at the private residence network, and a printer to be used with the workstation. CX0725; CX0727.[25]

2. Operation of the Network

LabMD's network included a number of servers that hosted applications, including back-up, email, webserver, database, laboratory, and billing applications. CX0740 (Hill) ¶ 39; CX0202; CX0711; CX0707; CX0552; CX0734; CX0584; CX0705.[26] Some of these servers hosted multiple applications and also stored Personal Information. CX0740 (Hill) ¶ 39;

[21] CX0705 (Bradley Dep. Tr.) at 20; CX0725 (Martin Dep. Tr.) at 11; CX0727 (Parr Dep. Tr.) at 44-45.

[22] CX0725 (Martin Dep. Tr.) at 12-13; CX0727 (Parr Dep. Tr.) at 44-46.

[23] CX0725 (Martin Dep. Tr.) at 11, 16-17; CX0727 (Parr Dep. Tr.) at 50; CX0709 (Daugherty Dep. Tr.) at 59.

[24] CX0705 (Bradley Dep. Tr.) at 22, 28, 29; CX0725 (Martin Dep. Tr.) at 11-13, 16-17, 19, 108-111; CX0727 (Parr Dep. Tr.) at 45-46, 48-49.

[25] CX0725 (Martin Dep. Tr.) at 16-18; CX0727 (Parr Dep. Tr.) at 50.

[26] CX0202 (Network Diagram – Drawn by Jeremy Dooley at Deposition); CX0711 (Dooley Dep. Tr.) at 22-29 (describing applications on Respondent's network at Respondent's Perimeter Center location); CX0707 (Bureau Dep. Tr.) at 63-64 (noting email and laboratory applications on servers on Respondent's network); CX0552 (Network Diagram Hand-drawn at Simmons IH); CX0734 (Simmons Invest. Hrg. Tr). at 32-40; CX0584 (Network Diagram Hand-drawn at Kaloustian IH); CX0735 (Kaloustian Invest. Hrg. Tr.) at 48-61; CX0705 (Bradley Dep. Tr.) at 24 (noting servers on Respondent's network at Respondent's Powers Ferry Road Location).

CX0735; CX0711.[27] For example, one server hosted billing and mail applications. CX0740 (Hill) ¶ 39; CX0034; CX0735.[28]

LabMD provided computers to physician clients. CX0740 (Hill) ¶ 33; CX0718; CX0728; CX0726; CX0725; CX0730; CX0722.[29] Physician clients sent Personal Information over the Internet to LabMD through these computers. CX0740 (Hill) ¶ 33; CX0730; CX0728; CX0726; CX0727; CX0225.[30] The Personal Information LabMD received from physician clients typically was transmitted from physician clients to LabMD's network using a File Transfer Protocol (FTP) service LabMD installed on its network and the computers it provided to physician offices. CX0740 (Hill) ¶ 34; CX0730; CX0710; CX0711; CX0717; CX0724; CX0725.[31]

The Personal Information physicians sent to LabMD included names, addresses, Social Security numbers, insurance information, diagnosis codes, physician orders for tests and

[27] CX0735 (Kaloustian Invest. Hrg. Tr.) at 48-61; CX0711 (Dooley Dep. Tr.) at 28-29.

[28] CX0034 (Network Diagrams – Perimeter Center West Location & Powers Ferry Road Location); CX0735 (Kaloustian Invest. Hrg. Tr.) at 57-59.

[29] CX0718 (Hudson Dep. Tr.) at 75; CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 21-22, 32-33; CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 26-29; CX0725 (Martin Dep. Tr.) at 56-57 (noting that Respondent provided hardware to physician offices); CX0730 (Simmons Dep. Tr.) at 61-62; CX0722 (Knox Dep. Tr.) at 64.

[30] CX0730 (Simmons Dep. Tr.) at 61-62; CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 47-48; CX0727 (Parr Dep. Tr.) at 21-22 (describing transfer of patient demographic information from physician office to Respondent's system); CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 39-43; CX0225 (Ltr. from Maxey, Southeast Urology Network) at 1-2 (explaining that LabMD's computer equipment facilitated "lab ordering and tracking lab results" including by downloading "S.U.N.'s patients' demographic and insurance information to LabMD's server in Atlanta").

[31] CX0730 (Simmons Dep. Tr.) at 61; CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 168; CX0711 (Dooley Dep. Tr.) at 131-32; CX0717 (Howard Dep. Tr.) at 34-35; CX0724 (Maire Dep. Tr.) at 41-42; CX0725 (Martin Dep. Tr.) at 56-60.

services, and other information. CX0740 (Hill) ¶ 33; CX0735; CX0717; CX0726; CX0728.[32] In some instances, physician clients entered the information into the computer that LabMD had provided, one consumer at a time, and then sent the information to LabMD. CX0740 (Hill) ¶ 33; CX0717; CX0728; CX0725; CX0726.[33] In other instances, the computer belonging to LabMD in the physician's office retrieved Personal Information for *all* patients of the physician's practice from a database located on another computer in the physician's office and forwarded the information for all of those patients in bulk to LabMD, regardless of whether LabMD performed testing for those patients. CX0740 (Hill) ¶ 33; CX0730; CX0725; CX0718; CX0717.[34]

Whether Personal Information came as a bulk transfer or one consumer at a time, it was received by a server on LabMD's network called Mapper, where it was processed so that it could be used by applications LabMD used in its laboratory and billing department and then maintained on servers on the network. CX0740 (Hill) ¶ 35; CX0735; CX0725; CX0704; CX0711; CX0719.[35] The laboratory and billing applications also ran on servers on LabMD's

[32] CX0735 (Kaloustian Invest. Hrg. Tr.) at 53-55; CX0717 (Howard Dep. Tr.) at 34-38; CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 41-42; CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 47-48.

[33] CX0717 (Howard Dep. Tr.) at 34-37 (explaining how some physician clients of Respondent transmitted patient data to Respondent); CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 50-52; CX0725 (Martin Dep. Tr.) at 61-62; (describing how phlebotomist manually entered information into web portal); CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 39-43.

[34] CX0730 (Simmons Dep. Tr.) at 60-65; CX0725 (Martin Dep. Tr.) at 58; CX0718 (Hudson Dep. Tr.) at 24-25, 40, 53-54; CX0717 (Howard Dep. Tr.) at 33-38.

[35] CX0735 (Kaloustian Invest. Hrg. Tr.) at 51-52, 225, 302; CX0725 (Martin Dep. Tr.) at 82-83; CX0704 (Boyle Dep. Tr.) at 24; CX0711 (Dooley Dep. Tr.) at 28-29, 131-33; CX0719 (Hyer Dep. Tr.) at 108-09.

network. CX0740 (Hill) ¶ 35; CX0735; CX0702; CX0725.[36] In addition, LabMD maintained Personal Information on desktop computers, such as the finance/billing manager's computer. CX0740 (Hill) ¶ 35; CX0702; CX0725; CX0735.[37] After LabMD's laboratory and medical employees had provided the services ordered by physician clients, they added results to the Personal Information Respondent maintained on its network. CX0740 (Hill) ¶ 36; CX0710; CX0717.[38] LabMD did not encrypt Personal Information while it was maintained on its network. CX0740 (Hill) ¶ 37; CX0734; CX0735.[39]

Physician clients typically retrieved the results of the services they ordered from LabMD through its web portal. CX0740 (Hill) ¶ 38; CX0735; CX0704; CX0722; CX0717.[40] In doing so, they accessed Personal Information stored on LabMD's network. CX0740 (Hill) ¶ 38; CX0704; CX0711.[41]

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

---

[36] CX0735 (Kaloustian Invest. Hrg. Tr.) at 50-55; CX0702 (Network Diagram 3 Hand-drawn at Martin Deposition); CX0725 (Martin Dep. Tr.) at 174-75 (describing flow of information from Labnet application to billing application).

[37] CX0702 (Network Diagram 2 Hand-drawn at Martin Deposition); CX0725 (Martin Dep. Tr.) at 174-76; CX0735 (Kaloustian Invest. Hrg. Tr.) at 117-20.

[38] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 193; CX0717 (Howard Dep. Tr.) at 49. LabMD also received results from laboratories to which it outsourced tests. CX0737 (Hill Reb.) ¶ 17 & n.22; CX0735 (Kaloustian Invest. Hrg. Tr.) at 100.

[39] CX0734 (Simmons Invest. Hrg. Tr.) at 43; CX0735 (Kaloustian Invest. Hrg. Tr.) at 53 (describing Personal Information in Mapper system), 62 (stating that personal information of patients in Mapper system was not encrypted).

[40] CX0735 (Kaloustian Invest. Hrg. Tr.) at 302-03; CX0704, 16, 22, 33 (Boyle Dep. Tr.) at 16, 22, 23; CX0722 (Knox Dep. Tr.) at 76-78; CX0717 (Howard Dep. Tr.) at 59-60.

[41] CX0704 (Boyle Dep. Tr.) at 33; CX0711 (Dooley Dep. Tr.) at 131-32 (describing life cycle of patient data).

provided access to Personal Information maintained on the network. CX0740 (Hill) ¶ 40; CX0735; CX0706; CX0714; CX0716.[42] Some LabMD employees could remotely access Respondent's network, including Personal Information maintained on the network. CX0740 (Hill) ¶ 40; CX0737 (Hill Reb.) ¶ 17 & n.20; CX0730; CX0711; CX0715; CX0706.[43]

C. Peer-to-Peer File Sharing Applications

1. Operation of Peer-to-Peer File-Sharing Applications

Peer-to-peer (P2P) file sharing applications are software programs that run on computers. CX0738 (Shields) ¶¶ 14-15. P2P file sharing applications, of which LimeWire is an example, are often used to share music, videos, pictures, and other materials stored on a consumer's computer with other users. Ans. ¶ 13; CX0738 (Shields) ¶ 14; CX0730; CX0704, CX0731.[44] The computers that run P2P applications are referred to as "peers" or "nodes," and each peer participates in the network, communicating over the Internet using a specific protocol or set of rules.[45] CX0738 (Shields) ¶ 15. The sharing of these materials occurs between persons and entities using computers with the same application or compatible P2P applications, which

[42] CX0735 (Kaloustian Invest. Hrg. Tr.) at 233-34, 241-242; CX0706 (Brown Dep. Tr.) at 117-19; CX0714 (Former LabMD Employee Dep. Tr.) at 41-45; CX0716 (Harris Dep. Tr.) at 72-73. Those applications included LabSoft, LabMD's laboratory application, and Lytec, LabMD's billing application.

[43] CX0730 (Simmons Dep. Tr.) at 50-53; CX0711 (Dooley Dep. Tr.) at 60-61; CX0715 (Gilbreth Dep. Tr.) at 61-63; CX0706 (Brown Dep. Tr.) at 7-12.

[44] CX0730 (Simmons Dep. Tr.) at 100; CX0704 (Boyle Dep. Tr.) at 62, 81-87; CX0731 (Truett Dep. Tr.) at 104-05.

[45] For example, the Gnutella protocol for searching was originally set up such that a user would initiate a search request by choosing some search criteria. The Gnutella software running on the user's computer would then create and send a search request using those criteria. A peer that received a query would forward it on to all the other peers to which it was connected, each time it was forwarded being called a "hop." A peer that had a file that matched the query would then send a reply back to the requestor. The user could then review the search responses and could choose to download one of the files. CX0738 (Shields) ¶ 23.

together make up the P2P network. CX0738 (Shields) ¶¶ 14-15; Ans. ¶ 13.[46] Each P2P network runs on a specific protocol; specifically, the P2P application LimeWire runs on the Gnutella protocol. CX0738 (Shields) ¶¶ 15, 17. Each P2P application that uses Gnutella is part of the same P2P network as LimeWire. CX0738 (Shields) ¶¶ 14, 15, 17; CX0950 (Fisk) at 9.

P2P applications allow a user to designate files on the user's computer to be available to others on a P2P network. CX0738 (Shields) ¶¶ 17, 22; CX0740 (Hill) ¶ 42; CX0730; CX0731.[47] P2P programs, including LimeWire, are designed to offer access to a set of files on the user's computer to other users of the P2P network. CX0738 (Shields) ¶ 14. When installing the program, the user is required to select a folder or folders on his or her computer to share on the P2P network. CX0738 (Shields) ¶ 17. Commonly, the folder that is selected to receive downloads from the P2P network is also the folder designated by the user to be shared with others on the network. CX0738 (Shields) ¶ 20.

P2P applications also allow a user to search for and access designated files on other computers on the P2P network. CX0738 (Shields) ¶¶ 14, 18, 31, 56-57, 65, 69-71; CX0950 (Fisk) at 9; CX0703; CX0730.[48] LimeWire users, or "peers," can search the Gnutella P2P network in a number of ways. Peers can search for a particular file of interest using its file name, such as "W-9 Form," CX0738 (Shields) ¶¶ 30, 58, or its "hash" value, CX0738 (Shields) ¶ 28.[49]

---

[46] Ans. ¶ 13 admits this allegation of the Complaint.

[47] CX0730 (Simmons Dep. Tr.) at 12; CX0731 (Truett Dep. Tr.) at 104-06.

[48] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 31 (explaining that P2P network works by searching computers connected to the network with the file-sharing software running); CX0730 (Simmons Dep. Tr.) at 12.

[49] A "hash" is a long number computed based on all data that makes up the file. The hash is statistically unique to that file, and is essentially impossible to forge. CX0738 (Shields) ¶ 28. A "hash search" allows a user to search for

Peers also can search using file extensions, such as "pdf" (CX0738 (Shields) ¶ 69), and sort through the search results to find interesting files. Even without searching for a particular file of interest or conducting a file extension search, a user may be able to find files made available by another peer by searching for names of files commonly included in the Windows "My Documents" folder, if that folder has been designated for sharing.[50] CX0738 (Shields) ¶¶ 65-66. Regardless of the method by which a user has reached another peer's sharing folder, once there, the user can invoke LimeWire's "browse host" function to get a list of all the other files the peer has available. CX0738 (Shields) ¶¶ 29, 56-57; CX0950 (Fisk) at 16. A user searching by any one of these methods will then select the file he or she wants to download, and the file will be downloaded from the peer(s) that are sharing the file to the user's computer. CX0738 (Shields) ¶ 18.

After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. CX0738 (Shields) ¶ 21; CX0740 (Hill) ¶ 44; CX0703.[51] Because of this re-sharing model, generally a file cannot with certainty be removed permanently from a P2P network once it has been shared. CX0738 (Shields) ¶ 21; CX0740 (Hill) ¶ 44.

---

a specific file using a hash to find other peers that are sharing the identical file. CX0738 (Shields) ¶ 28; CX0703; CX0721; CX0703 (Tiversa Dep. Tr.) at 41-42, 73-74; CX0721 (Johnson Dep. Tr.) at 114-15.

[50] At the time when LimeWire was installed on Respondent's computer (in 2005 or 2006), *see infra* Section IV.D.1, using a commonly-used directory such as the "My Documents" folder for file sharing was a known problem and was common enough that LimeWire added a warning to notify users when they were sharing the folder. CX0738 (Shields) ¶ 38.

[51] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 20-21.

2. Risk of Inadvertent Sharing through Peer-to-Peer File Sharing Applications

Security professionals and others, including the Commission, have warned for years about the risks of P2P file sharing, and this information was well-known among security professionals since at least 2005. Research on the inadvertent sharing of Personal Information through P2P networks was publicly released starting as early as 2002. CX0738 (Shields) ¶¶ 40-44; CX0874; CX0875; CX0876; CX0877.[52] In 2005, the US Computer Emergency Readiness Team, a government agency that provides information to security professionals and the public on cybersecurity issues, warned that through P2P sharing "unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information." CX0738 (Shields) ¶ 46; CX0878.[53]

The Commission has engaged in extensive consumer and business education on the risks of sharing Personal Information through the use of P2P software, as well as issuing a report and testifying before Congress on numerous occasions to provide information on the subject. In 2003, the Commission distributed a consumer alert publication called "File-Sharing: A Fair Share? Maybe Not," which cautioned "when you are connected to file-sharing programs, you may unknowingly allow others to copy private files you never intended to share," providing as

[52] CX0874 (SANS Institute InfoSec Reading Room Peer-to-Peer File-Sharing Networks Security) at 6, 11 (describing risk of inadvertent sharing posed by P2P software in 2002); CX0875(Security Implications of "Peer-To-Peer" Software) at 4 (2002); CX0876 (Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications) at 14 (2003); CX0877 (Peer-to-Peer (P2P) File Sharing Applications and their Threat to the Corporate Environment) at 8 (2003).

[53] CX0878 (US-CERT - Risks of File-Sharing Technology) at 1; *see also* CX0879 (Secure Anchor - Security Best Practices) at 2 (listing peer-to-peer file sharing as an activity that may be prohibited as a security best practice).

examples, "tax returns, email messages, *medical records*, photos, or other personal documents." CX0770 (emphasis added).[54] The Commission reiterated this message in similar June 2005, July 2005, December 2005, and April 2008 consumer alerts, as well as in August 2005 and February 2007 Spanish language alerts. CX0778; CX0779; CX0784; CX0788; CX0780; CX0785; CX0789.[55] In September 2005, the Commission issued a broader online security publication for consumers, "Stop. Think. Click.," which contained similar P2P warnings (CX0781[56]), distributing it in Spanish in October and November 2005 (CX0782; CX0783[57]). On the business education side, in a 2004 joint business alert issued with the Council of Better Business Bureaus and the National Cyber Security Alliance, the FTC included a warning about the risks of file-sharing, urging that "[u]nless there's a business reason to share files, consider turning off this function and prohibiting your employees from installing file-sharing programs on their computers." CX0771.[58]

In testifying before Congress on May 6, 2004 and again on June 23, 2004, the Commission noted that P2P software presents a risk that sensitive personal files may be

[54] CX0770 (FTC Consumer Alert: File-Sharing: A Fair Share? Maybe Not.) at 2, 4 (emphasis added).

[55] CX0778 (Revised FTC Consumer Alert: P2P File-Sharing: Evaluating the Risks) (June 2005); CX0779 (Revised FTC Consumer Alert: P2P File-Sharing: Evaluate the Risks) (July 2005); CX0784 (FTC Distribution: Revised P2P File Sharing: Evaluate the Risks) (Dec. 2006); CX0788 (FTC Distribution: Revised P2P File Sharing: Evaluate the Risks) (April 2008); CX0780 (Revised FTC Spanish Consumer Alert: File-Sharing: Evaluating the Risks) (Spanish Aug. 2005); CX0785 (Revised FTC Spanish Consumer Alert: File-Sharing: Evaluating the Risks) (Spanish Feb. 2007); CX0789 (Revised FTC Spanish Consumer Alert: File-Sharing: Evaluate the Risks) (Spanish April 2008).

[56] CX0781 (FTC Distribution: Stop.Think.Click: 7 Practices for Safer Computing) at 5.

[57] CX0782 (FTC Spanish Distribution: Stop. Think. Click brochure) at 7; CX0783 (FTC Spanish Distribution: New version of Stop. Think. Click brochure) at 5.

[58] 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.

disclosed inadvertently. CX0773, CX0775.[59] In June 2005, Commission staff issued a report on P2P technology; it included a section discussing the risk of unintentional sharing of files containing Personal Information, and warned that "[i]nadvertent sharing can have significant irremediable effects: once Personal Information is shared, a user cannot retrieve it." CX0777.[60] The Commission testified again before Congress in July 2007, repeatedly referring to the danger of sharing files beyond those intended. CX0787.[61] In that testimony the Commission described its consumer education efforts on the risks of P2P file sharing and other online dangers, and noted that its OnGuardOnline.gov website, which contained information on P2P, was visited by 250,000 consumers each month. *Id.*[62]

III. RESPONDENT'S ACTS OR PRACTICES WERE IN OR AFFECTING COMMERCE

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. This definition captures Respondent's business practices, as Respondent has admitted that it tested samples from states outside of Georgia, including

[59] CX0773 (Prepared Statement of FTC: Hearing on Online Pornography: Closing the Door on Pervasive Smut) at 7-8; CX0775 (Prepared Statement of FTC: Hearing on P2P File-Sharing Technology) at 4.

[60] CX0777 (FTC Staff Report: Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues) at 14.

[61] CX0787 (Prepared Statement of FTC on Peer-To-Peer File-Sharing Technology Issues) at 3 (consumers may unintentionally share personal or sensitive information); 6 n.9 (summarizing best practices Commission recommended to P2P software providers, including confirmation of which folders the user wishes to make available to others).

[62] *Id.* at 9-11 (describing consumer education efforts on file sharing).

Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona. Ans. ¶ 5; CX0766.[63] Furthermore, the consumers whose samples Respondent tested and from whom Respondent collects payments are "located throughout the United States." CX0766; CX0088; CX0726; CX0718; CX0722; CX0706; CX0715; CX0713; CX0714.[64] 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 State and Respondent's admission that LabMD tests 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 scope of operations imparted the requisite interstate character).

IV. LABMD'S MEASURES TO PROTECT PERSONAL INFORMATION ON ITS NETWORK WERE NOT REASONABLE OR APPROPRIATE

A. Legal Standard Under Section 5: Reasonable Security

The Complaint alleges that Respondent's conduct was unfair, in violation of Section 5 of the FTC Act. The statutory text of the FTC Act confers broad power to the Commission to protect consumers from "unfair or deceptive acts or practices." 15 U.S.C. § 45. Congress deliberately delegated broad power to the FTC under Section 5 of the FTC Act to address

[63] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admissions 7-12 (tested specimens of consumers and provided test results to physicians located in at least seven states).

[64] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admissions 10-12, 29-33; CX0088 (copies of check made payable to LabMD from consumers in various states, found by the Sacramento Police Department in October 2012); CX0726 (Maxey, Designee of Southeast Urology Network, Dep. Tr.) at 17, 21; CX0718 (Hudson Dep. Tr.) at 15-17; CX0722 (Knox Dep. Tr.) at 19; CX0706 (Brown Dep. Tr.) at 16-18; CX0715 (Gilbreth Dep. Tr.) at 50-51; CX0713 (Gardner Dep. Tr.) at 25-26; CX0714 (Former LabMD Employee Dep. Tr.) at 15-16.

unanticipated practices in a changing economy. *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972). Congress has defined an unfair practice as one that "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The codification of unfairness established a cost-benefit analysis to evaluate whether practices are unfair. 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.").

Applied to data security, the unfairness analysis begins with an assessment of consumer injuries that may result from a company's information security practices. As the Commission has made clear, 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 on Resp't's Mot. to Dismiss at 19 ("[O]ccurrences 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). Instead, this inquiry turns on whether the unauthorized disclosure of Personal Information held by a company caused or is likely to cause consumer harm. *Id.* at 18-19 (requiring assessment of whether a company's "data security procedures were

'unreasonable' in light of the circumstances"). The second consideration is whether consumers could have avoided the likely harms resulting from the company's unauthorized disclosure. *Id.* at 19. Finally, unfairness requires an evaluation of whether the company's security practices benefit consumers or competition. *Id.* Countervailing benefits are unlikely to be significant when more effective security measures could have been implemented at relatively low cost. As the Commission recently expressed it: "the touchstone of the Commission's approach to data security is reasonableness." Comm'n Statement Marking 50th Data Sec. Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.[65]

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

[65] The unfairness cases include: *In re Accretive Health, Inc.*, FTC Docket No. C-4432, FTC File No. 122-3077 (Feb. 24, 2014) (consent order); *In re Genelink and foru Int'l Corp.*, FTC File No. 112-3095 (Jan. 7, 2014) (consent order); *In re GMR Transcription Svcs., Inc.*, FTC File No. 122-3095 (Jan. 31, 2014) (consent order); *In re TRENDnet, Inc.*, FTC Docket No. C-4426, FTC File No. 122 3090 (Jan. 16, 2014); *In re HTC America, Inc.*, FTC Docket No. C-4406, FTC File No. 122-3049 (June 25, 2013) (consent order); *In re Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (Feb. 20, 2013) (consent order); *In re EPN, Inc.*, FTC Docket No. C-4370, FTC File No. 112-3143 (Oct. 3, 2012) (consent order); *FTC v. Wyndham Worldwide Corp.*, No. 2:13-CV-01887 (D.N.J.) (pending litigation); *In re Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (Mar. 27, 2012) (consent order); *In re Lookout Servs., Inc.*, FTC Docket No. C-4326, FTC File No. 102-3076 (June 15, 2011) (consent order); *In re Ceridian Corp.*, FTC Docket No. C-4325, FTC File No. 102-3160 (June 8, 2011) (consent order); *In re Rite Aid Corp.*, FTC Docket No. C-4308, FTC File No. 072-3121 (Nov. 12, 2010) (consent order); *In re Dave & Buster's, Inc.*, FTC Docket No. C-4291, FTC File No. 082-3153 (May 20, 2010) (consent order); *United States v. Rental Research Servs., Inc.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *In re CVS Caremark Corp.*, FTC Docket No. C-4259, FTC File No. 72-3119 (June 18, 2009) (consent order); *In re The TJX Cos.*, FTC Docket No. C-4227, FTC File No. 072-3055 (July 29, 2008) (consent order); *In re Reed Elsevier Inc.*, FTC Docket No. C4226, FTC File No. 052-3094 (July 29, 2008) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (consent order); *In re DSW Inc.*, FTC Docket No. C-4157, FTC File No. 052-3096 (Mar. 7, 2006) (consent order); *United States v. ChoicePoint Inc.*, FTC File No. 052-3069, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006) (stipulated final judgment); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (consent order).

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.*, No. 12-00325, 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).

Companies wishing to protect sensitive information, including Personal Information, have extensive guidance available on how to identify the risks and vulnerabilities they face, and select and maintain data security practices that are reasonable under their circumstances. 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. 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.[66] Similarly, the SANS Institute has since 2001

[66] Since 1990, NIST has published and updated a series of Special Publications ("SP-800") on information security topics. *See, e.g.*, NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

annually published and updated a free, easily accessible list of the most critical security vulnerabilities confronting firms, security professionals, and law enforcement.[67] 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.

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"), which 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

---

(Oct. 1995), *available at* http://csrc nist.gov/publications/nistpubs/800-12/800-12-html/; NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002; updated September 2012), *available at* http://csrc nist.gov/publications/nistpubs/800-30/sp800-30.pdf and http://csrc nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. Although prepared for government computer systems, these publications also provide guidance to the private sector.

[67] SANS Institute, The Top 20 Most Critical Internet Security Vulnerabilities (Updated) (November 2005), *available at* https://files.sans.org/top20/top20_2005.pdf (identifying file sharing applications as a critical vulnerability).

assessment would have revealed.[68] The consent decrees approved by the Commission in data security matters provide the same basic guidance by imposing relief that requires respondents to implement a comprehensive information security plan that includes these fundamental security elements.[69]

[68] *See In re GMR Transcription Svcs., Inc.*, FTC File No. 122-3095 (Jan. 31, 2014) (consent order approved for public comment); *In re foruTM International Corp*., FTC File No. 122-3105 (April 14, 2014) (consent order approved for public comment); *In re of Genelink, Inc*., FTC File No.112-3095 (Jan. 15, 2014) (consent order approved for public comment); *In re TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013) (consent order approved for public comment); *In re of HTC America Inc.*, FTC Docket No. C-4406, FTC File No. 122-3049 (June 25, 2013) (consent order); *In re Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (Feb. 20, 2013) (consent order); *In re of EPN, Inc.*, FTC Docket No. C-4370, FTC File No. 112-3143 (Oct. 3, 2012) (consent order); *In re Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (Mar. 27, 2012) (consent order); *In re Lookout Servs., Inc.*, FTC Docket No. C-4326, FTC File No. 102-3076 (June 15, 2011) (consent order); *In re Ceridian Corp.*, FTC Docket No. C-4325, FTC File No. 102-3160 (June 8, 2011) (consent order); *In re Rite Aid Corp.*, FTC Docket No. C-4308, FTC File No. 072-3121 (Nov. 12, 2010) (consent order); *In re CVS Caremark Corp.*, FTC Docket No. C-4259, FTC File No. 72-3119 (June 18, 2009) (consent order); *In re Reed Elsevier Inc.*, FTC File No. 052-3094 (July 29, 2008) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (consent order) (all alleging some form of risk assessment failure).

[69] See *In re GMR Transcription Svcs, Inc*., FTC File No. 122-3095 (Jan. 31, 2014) (consent order approved for public comment); *In re foruTM International Corp*., FTC File No. 122-3105 (April 14, 2014) (consent order approved for public comment); *In re Genelink, Inc*., FTC File No.112-3095 (Jan. 15, 2014) (consent order approved for public comment); *In re Accretive Health, Inc*., FTC File No. 122-3077 (Feb. 24, 2014); *In re TRENDnet, Inc.*, FTC File No. 122 3090 (Sept. 4, 2013) (consent order approved for public comment); *In re HTC America Inc.*, FTC Docket No. C-4406, FTC File No. 122-3049 (June 25, 2013) (consent order); *In re Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (Feb. 20, 2013) (consent order); *In re EPN, Inc.*, FTC Docket No. C-4370, FTC File No. 112-3143 (Oct. 3, 2012) (consent order); *In re Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (Mar. 27, 2012) (consent order); *In re Lookout Servs., Inc.*, FTC Docket No. C-4326, FTC File No. 102-3076 (June 15, 2011) (consent order); *In re Ceridian Corp.*, FTC Docket No. C-4325, FTC File No. 102-3160 (June 8, 2011) (consent order); *In re Rite Aid Corp.*, FTC Docket No. C-4308, FTC File No. 072-3121 (Nov. 12, 2010) (consent order); *In re Dave & Buster's, Inc.*, FTC Docket No. C-4291, FTC File No. 082-3153 (May 20, 2010) (consent order); *United States v. Rental Research Servs.*, No. 0:09-CV-00524 (D. Minn. Mar. 6, 2009) (stipulated order); *In re CVS Caremark Corp.*, FTC Docket No. C-4259, FTC File No. 72-3119 (Jun. 18, 2009) (consent order); *In re The TJX Cos.*, FTC Docket No. C-4227, FTC File No. 072-3055 (July 29, 2008) (consent order); *In re Reed Elsevier Inc.*, FTC File No. 052-3094 (July 29, 2008) (consent order); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (consent order); *In re DSW, Inc.*, FTC Docket No. C-4157, FTC File No. 052-3096 (Mar. 7, 2006) (consent order); *United States v. ChoicePoint, Inc.*, FTC File No. 052-3069, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006) (stipulated final judgment); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (consent order).

B. LabMD Failed to Provide Reasonable and Appropriate Security for Personal Information on its Computer Networks

As alleged in Paragraph 10 of the Complaint, LabMD engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for Personal Information on its computer networks. The expert reports of Professor Hill and the testimony of LabMD's former employees illustrate LabMD's failures. CX0740 (Hill); CX0737 (Hill Reb.); CX0704; CX0705; CX0706; CX0707; CX0708; CX0709; CX0710; CX0711; CX0713; CX0714; CX0715; CX0716; CX0717; CX0718; CX0719; CX0721; CX0722; CX0724; CX0725; CX0727; CX0730; CX0733; CX0734; CX0735; CX0736.[70]

LabMD failed to use a comprehensive, layered approach to security, also known as "defense in depth." CX0740 (Hill) ¶¶ 27-30; CX0737 (Hill Reb.) ¶¶ 7-12. Defense in depth is the most effective way to reasonably secure a network. CX0740 (Hill) ¶ 27; CX0737 (Hill Reb.) ¶ 7. It reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple security measures deployed at different layers of the network. CX0740 (Hill) ¶¶ 27-30; CX0737 (Hill Reb.) ¶¶ 7-8. Implementing a defense in depth strategy 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

[70] CX0704 (Boyle Dep. Tr.); CX0705 (Bradley Dep. Tr.); CX0706 (Brown Dep. Tr.); CX0707 (Bureau Dep. Tr.); CX0709 (Daugherty Dep. Tr.); CX0710 (Daugherty, LabMD Designee, Dep. Tr.); CX0711 (Dooley Dep. Tr.); CX0713 (Gardner Dep. Tr.); CX0714 (Former LabMD Employee Dep. Tr.); CX0715 (Gilbreth Dep. Tr.); CX0716 (Harris Dep. Tr.); CX0717 (Howard Dep. Tr.); CX0718 (Hudson Dep. Tr.); CX0719 (Hyer Dep. Tr.); CX0722 (Knox Dep. Tr.); CX0724 (Maire Dep. Tr.); CX0725 (Martin Dep. Tr.); CX0727 (Parr Dep. Tr.); CX0730 (Simmons Dep. Tr.); CX0733 (Boyle, LabMD Designee, Invest. Hrg. Tr.); CX0734 (Simmons Invest. Hrg. Tr.); CX0735 (Kaloustian Invest. Hrg. Tr.); CX0736 (Daugherty Invest. Hrg. Tr.).

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

Professor Hill's report explains that, when implementing a defense in depth 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; and (6) Probe the network with periodic audits, including penetration testing. CX0740 (Hill) ¶ 31. Professor Hill further explains that an appropriate defense in depth 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 within 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) ¶¶ 27-30, 75; CX0737 (Hill Reb.) ¶¶ 7-9.

As described below, LabMD did not implement a defense in depth strategy. Specifically, LabMD did not have a comprehensive information security program; it failed to conduct risk assessments; it did not prevent employees from accessing unnecessary Personal Information; it failed to use common authentication techniques; it did not update its operating systems; and it failed to prevent or detect unauthorized access to Personal Information on its computer networks, which resulted in LabMD not detecting the installation or use of an unauthorized file sharing application on its networks. Its failures in this regard resulted in Personal Information for more than 750,000 consumers being inadequately protected from unauthorized disclosure.

1. LabMD Did Not Have a Comprehensive Information Security Program

LabMD did not develop, implement, or maintain a comprehensive information security program to protect consumers' Personal Information. CX0740 (Hill) ¶ 61. 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; the written policies that satisfy those goals; and the mechanisms that enforce the written policies. CX0740 (Hill) ¶ 52-57; CX0737 (Hill Reb.) ¶ 7. *Ad hoc*, informal policies are insufficient to implement a comprehensive information security program. Rather, written policies are necessary to provide guidance to the employees responsible for implementing the plan and to those who must comply with them. CX0740 (Hill) ¶ 53; CX0737 (Hill Reb.) ¶ 26. Reducing policies to writing also permits a company to transition responsibility for information security when there are personnel changes and to adapt the company's goals as security threats evolve. *Id.*

From 2005 through 2010, LabMD had no written information security program. CX0740 (Hill) ¶ 61(a); CX0733.[71] The only written document that existed that related, however tangentially, to information security was an employee handbook, which identified one compliance goal related to confidentiality but did not explain what, if any, mechanisms LabMD implemented to achieve the goal. CX0740 (Hill) ¶ 61(a); CX001; CX002.[72] In addition, not a

[71] CX0733 (Boyle Invest. Hrg. Tr.) at 78-79, 91-92.

[72] CX0001 (LabMD Employee Handbook Rev. June 2004) at 5-6; CX0002 (LabMD Employee Handbook Rev. Mar. 2008) at 5-6 (both stating that LabMD takes "specific measures" to protect personal information from sharing and indicating that employees will "learn more," but providing no additional information).

single employee—including LabMD's CEO—could describe what mechanisms LabMD implemented to achieve the stated compliance goal. CX0725; CX0711; CX0719; CX0704; CX0710.[73]

In 2010, LabMD reduced its purported policies to two written policy manuals. CX0733; CX006; CX007.[74] LabMD contends that one set of policies it memorialized in 2010 was in place in 2007 and 2008. CX0733.[75] However, there is no documentation establishing that LabMD had been implementing those policies. CX0740 (Hill) ¶ 61(b); CX0733.[76] Furthermore, to the extent that the purported policies were allegedly implemented prior to 2010, some were not being enforced. CX0740 (Hill) ¶ 61(b). For example, if LabMD's purported policy to identify and remove unauthorized software had been implemented (CX0006; CX0007[77]), unauthorized software would have been detected and removed from employee computers. CX0740 (Hill) ¶ 61(b). However, for a period of as long as three years, an employee with access to sensitive Personal Information for hundreds of thousands of consumers had installed and used an unauthorized P2P file sharing program. CX0755; CX0766.[78] LabMD's processes did not detect

[73] CX0725 (Martin Dep. Tr.) at 166-67; CX0711 (Dooley Dep. Tr.) at 144-45; CX0719 (Hyer Dep. Tr.) at 162-63; CX0710 (Boyle Invest. Hrg. Tr.) at 248-49; CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 119 (stating that employee handbook not specific on security measures); 135-37 (stating company has no documentation of measures taken to comply with HIPAA).

[74] CX0733 (Boyle Invest. Hrg. Tr.) at 78-79, 91-92, 97-98; CX006 (LabMD Policy Manual); CX007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual).

[75] CX0733 (Boyle Invest. Hrg. Tr.) at 78-79, 91-92, 97-98.

[76] CX0733 (Boyle Invest. Hrg. Tr.) at 78-79.

[77] CX0006 (LabMD Policy Manual) at 18; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 31.

[78] CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) Interrog. 3 (LimeWire was downloaded to a LabMD computer in or about 2005); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 40-

the software or prevent its use. CX0740 (Hill) ¶ 61(b); CX0735; CX0734; CX0730; CX0711; CX0717; CX0719.[79] Similarly, LabMD did not provide its staff with the encryption tools identified in its purported policy (CX0006; CX0007; CX0711; CX0707; CX0713; CX0718; CX0722; CX0735; CX0734; CX0709[80]), nor did it provide its staff with training on how to secure sensitive information included in emails or attachments (CX0711**;** CX0707; CX0713; CX0718[81]).

Not only did LabMD delay in creating written policies and fail to enforce those policies, its 2010 Policy Manual and its Computer Hardware, Software and Data Usage and Security Policy Manual are not sufficiently comprehensive to adequately protect consumers' Personal Information. CX0740 (Hill) ¶ 61(c). For example, the policies do not specify how LabMD protects consumers' Personal Information transmitted between the physician offices and

---

41, 43-46 (LimeWire was not detected on a LabMD computer prior to May 2008), 35-36 (billing department computers used to process personal information).

[79] CX0735 (Kaloustian Invest. Hrg. Tr.) at 269-70 (stating that LabMD did not have capability to detect the installation or use of P2P software); CX0734 (Simmons Invest. Hrg. Tr.) at 160-61 (stating that LabMD did not have capability to detect the installation or use of P2P software); CX0730 (Simmons Dep. Tr.) at 53-56 (stating that LabMD did not have the capability to prevent installation of P2P software by some employees, and did not have the capability to detect installation or use of P2P software); CX0711 (Dooley Dep. Tr.) at 117-20 (stating that LabMD did not have capability to detect the installation or use of P2P software); CX0717 (Howard Dep. Tr.) at 146 (stating that he would not know if there was P2P software on a billing computer); CX0719 (Hyer Dep. Tr.) at 27-29, 33-34 (stating that prior to summer 2009 employees had capability to install software on their computers).

[80] CX0006 (LabMD Policy Manual) at 6 and CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 7 (both stating email containing sensitive information should be sent encrypted using "S/MIME, PGP, etc."); CX0711 (Dooley Dep. Tr.) at 107-08; CX0707 (Bureau Dep. Tr.) at 87-88; CX0713 (Gardner Dep. Tr.) at 62; CX0718 (Hudson Dep. Tr.) at 189; CX0735 (Kaloustian Invest. Hrg. Tr.) at 277; CX0734 (Simmons Invest. Hrg. Tr.) at 163; CX0722 (Knox Dep. Tr.) at 89; CX0709 (Daugherty Dep. Tr.) at 116-18 (didn't know if emails were encrypted).

[81] CX0711 (Dooley Dep. Tr.) at 107-08**;** CX0707 (Bureau Dep. Tr.) at 87-88; CX0713 (Gardner Dep. Tr.) at 62; CX0718 (Hudson Dep. Tr.) at 189

LabMD; nor do they dictate whether sensitive information should be stored in an encrypted format. CX0740 (Hill) ¶ 61(c); CX0006; CX0007.[82]

2. LabMD Did Not Use Appropriate, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities

LabMD did not use an appropriate set of readily available measures to assess risks and vulnerabilities to the Personal Information maintained on its computer network. CX0740 (Hill) ¶ 67. Risk assessments allow network administrators to choose security measures that are reasonable and appropriate under their circumstances. CX0740 (Hill) ¶¶ 64-66. Risk assessments are, therefore, an essential component of defense in depth. CX0740 (Hill) ¶ 64. LabMD did not implement risk assessment measures that were sufficient to identify or assess risks and vulnerabilities on its network. CX0740 (Hill) ¶ 67.

There are a variety of readily available means to identify, assess, and remediate risks. Examples include antivirus scans, firewall logs, vulnerability scans, intrusion detection systems, and penetration tests. CX0740 (Hill) ¶ 65. Each such measure typically evaluates a network's exposure to only one type of vulnerability. CX0740 (Hill) ¶ 63. For example, an antivirus application could assess the incidence of viruses on a network, but not the installation of unauthorized applications on the network. CX0740 (Hill) ¶ 65. Because no one mechanism can assess the exposure to all the risks and vulnerabilities a network may face, a number of mechanisms are required to adequately assess risks. CX0740 (Hill) ¶ 65. With information from

[82] CX0006 (LabMD Policy Manual) at 6; CX0007 (LabMD Computer Hardware, Software and Data Usage and Security Policy Manual) at 7 (both setting forth encryption policy for email but not addressing encryption in other

appropriate risk assessment measures, a company can make an informed decision about balancing the seriousness of a risk against the cost remediating the vulnerability. CX0740 (Hill) ¶ 75. As explained in Section IV.B, *supra*, the more sensitive the Personal Information maintained within the network, the greater the need for enhanced security measures. CX0740 (Hill) ¶ 75; CX0737 (Hill Reb.) ¶ 9.

LabMD implemented risk assessment mechanisms that were not sufficient to adequately identify or assess risks and vulnerabilities to the Personal Information maintained on its computer network. CX0740 (Hill) ¶¶ 67-69. Specifically, LabMD's limited antivirus applications, modest firewalls, and manual computer inspections were insufficient to evaluate risks to its computer network. CX0740 (Hill) ¶ 68.

The antivirus application LabMD used on critical servers did not always scan for viruses, and thus could not be relied upon to identify risks to the servers. CX0740 (Hill) ¶ 68(a); CX0035; CX0398.[83] Moreover, LabMD continued to use the same antivirus application after the vendor stopped providing updated virus definitions needed to identify newly discovered risks. CX0740 (Hill) ¶ 68(a); CX0398; CX0731.[84] On employee workstations, LabMD used antivirus applications that provided only limited risk assessment functionality, at least until 2006.

---

applications).

[83] CX0035 (APT Service Invoice) at 2 (noting that "labmdserver" could not run virus scan and virus definitions had not been updated for nearly a year, from July 2005 to May 2006); CX0398 (APT Service Invoice) at 4 (servers not updating antivirus definitions).

[84] CX0398 (APT Service Invoice) at 4 (servers running Symantec Corporate 7, which was no longer supported); CX0731 (Truett Dep. Tr.) at 82-84. Even after it implemented a more capable antivirus application, LabMD did not install it on all its equipment. CX0724 (Maire Dep. Tr.) at 94-95 (client computers not updated to new antivirus).

CX0740 (Hill) ¶ 68(a); CX0734.[85] These applications were not managed centrally by a network administrator; instead, LabMD relied upon individual employees to update the virus definitions on their computers and report warnings to LabMD's IT Department. CX0740 (Hill) ¶ 68(a); CX0735.[86]

The firewall product that LabMD used until 2010 (CX0710; CX0553[87]) could log only a very limited amount of information about online connections that had been made (CX0710[88]), and its memory could only store a few days' worth of such information at a time (CX0710; CX0731[89]). Instead of systematically reviewing logs before such stored information changed, LabMD's limited firewall logs were reviewed only to troubleshoot a performance problem, such as a user complaint that he or she could not connect to a website. CX0740 (Hill) ¶ 68(b); CX0731.[90] The firewall product could not monitor traffic, such as by automatically inspecting outbound traffic to determine if sensitive information was being exported from LabMD's network (CX0740 (Hill) ¶ 68(b); CX0711; CX0731[91]) and thus did not record results for review. LabMD's firewall product did not allow LabMD to see if sensitive information was being exported from its network without authorization, such as through a P2P file sharing program.

---

[85] CX0734 (Simmons Invest. Hrg. Tr.) at 87-88.

[86] CX0735 (Kaloustian Invest. Hrg.) at 126-32.

[87] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 177-78 (LabMD used ZyWALL firewall until it was replaced with Juniper firewall); CX0553 (MDS Juniper Proposal) (quote for Juniper firewall dated Aug. 18, 2010).

[88] CX 0731 (Truett Dep. Tr.) at 68.

[89] CX0710 (Daugherty, LabMD designee, Dep. Tr.) at 177; CX 0731 (Truett Dep. Tr.) at 69.

[90] CX0731 (Truett Dep. Tr.) at 68-69.

[91] CX0711 (Dooley Dep. Tr.) at 50-52; CX0731 (Truett Dep. Tr.) at 68 (ZyWALL firewall could only monitor connections, not traffic).

CX0735.[92] LabMD could have used free tools to do packet level analysis to provide information that could enable LabMD to determine if Personal Information left the network without authorization. CX0740 (Hill) ¶ 71.

LabMD claims that it used manual inspections to assess risks and vulnerabilities to the Personal Information maintained on its computer network. CX0710; CX0735.[93] Through at least mid-2008, however, LabMD employees performed manual computer inspections only in response to a physician or employee reporting that a computer had malfunctioned. CX0740 (Hill) ¶ 68(c); CX0735; CX0734; CX0707.[94] Even when conducted regularly and proactively, manual computer inspections are a poor substitute for automated tools because humans cannot inspect every place in a computer where risks and vulnerabilities can exist, and, even if they could, malicious software sometimes can mask its presence to avoid detection during a manual inspection. CX0740 (Hill) ¶ 68(c); CX0737 (Hill Reb.) ¶ 28.

LabMD did not implement an intrusion detection system. CX0740 (Hill) ¶ 69; CX0737 (Hill Reb.) ¶¶ 20, 23; CX0719; CX0731; CX0735; CX0717.[95] And LabMD did not conduct penetration tests until May 2010. CX0740 (Hill) ¶ 69; CX0710; CX0735; CX0719; CX0044;

[92] CX0735 (Kaloustian Invest. Hrg. Tr.) at 102.

[93] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 128-29, 137 (discussing "walk-arounds"); *see also* CX0735 (Kaloustian Invest. Hrg. Tr.) at 173-76 (automated tools not used to assess security of desktop computers), 205-06 (laptops); 296-97 (servers).

[94] CX0735 (Kaloustian Invest. Hrg. Tr.) at 177 (employees); CX0734 (Simmons. Invest. Hrg. Tr.) at 78-80 (employees), 85-86 (physicians); CX0707 (Bureau Dep. Tr.) at 50-52 (employees).

[95] CX0719 (Hyer Dep. Tr.) at 123-24, 126; CX0731 (Truett Dep. Tr.) at 122; CX0735 (Kaloustian Invest. Hrg. Tr.) at 92; CX0717 (Howard Dep. Tr.) at 58, 140.

CX0052.[96] Even then, LabMD's penetration tests were limited to external facing servers and did not test employee workstations and computers inside LabMD's network. CX0044.[97] LabMD could not adequately assess the extent of the risks and vulnerabilities of its network without using these automated mechanisms. CX0740 (Hill) ¶ 69. A penetration test of all IP addresses on the network, for example, would have identified vulnerabilities like outdated software, security patches that had not been applied, and administrative accounts with default settings. CX0740 (Hill) ¶ 70. Indeed, the external vulnerability scans 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) ¶ 72; CX0070.[98]

3. LabMD Did Not Use Adequate Measures to Prevent Employees From Accessing Personal Information Not Needed to Perform Their Jobs

LabMD failed to use adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs. CX0740 (Hill) ¶ 84. In addition, LabMD collected and maintained more data than LabMD required to conduct its business. CX0740 (Hill) ¶ 80(a). As a result, LabMD needlessly increased the scope of potential harm resulting from a network compromise.

---

[96] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 150-52; CX0735 (Kaloustian Invest. Hrg. Tr.) at 92, 282 (stating that no penetration tests were performed during his time at LabMD); CX0719 (Hyer Dep. Tr.) at 164, 175-76 ; CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 5 (authorizing performance of network testing on May 18, 2010); CX0052 (Final Page of ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty and H. Davidson).

[97] CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4 (listing locations to be tested).

[98] CX0070 (ProviDyn Network Security Scan – Mapper) at 19 (identifying Level 5 anonymous FTP server problem).

As part of a defense in depth strategy, companies that maintain sensitive information should restrict access to that data by defining roles for its employees and specifying the types of data that are needed by employees in those roles. CX0740 (Hill) ¶¶ 83, 85. 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) ¶ 81. Companies can use operating system functionalities and other applications to limit employees' access to information. CX0740 (Hill) ¶ 85.

LabMD is unable to specify the types of Personal Information that each of its employees was permitted to access via LabMD's network. CX0740 (Hill) ¶ 84(a); CX0754; Order on Mot. for Sanctions.[99] Rather, in response to an interrogatory regarding employees' access to Personal Information, LabMD could respond only that its employees had "various levels of access" to various types of Personal Information and that "all employees could gain knowledge of any Personal Information regarding Consumers to the extent it was necessary to the performance of their job duties." CX0740 (Hill) ¶ 84(a); CX0754.[100] If LabMD had implemented measures to limit its employees' access to Personal Information to *only* the types of Personal Information that the employees needed to perform their jobs, it would have been able to provide a more precise response to Complaint Counsel's Interrogatory. CX0740 (Hill) ¶ 84(b).

In addition to not implementing measures to limit its employees' access to Personal Information, LabMD maintained more information than it needed to conduct its business.

[99] CX0754 (LabMD's Supp. Resp. to First Set of Complaint Counsel's Interrogs. to Resp't) Interrog. 2; Order Granting in Part and Denying in Part Complaint Counsel's Mot. for Discovery Sanctions at 5 (Mar. 10, 2014).

CX0740 (Hill) ¶ 80(a). 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. CX0740 (Hill) ¶ 79. LabMD collected and maintained indefinitely Personal Information regarding approximately 100,000 consumers for whom it never performed testing. CX0766; CX0710; CX0718; CX0726.[101] Because LabMD never performed testing – directly, or indirectly by outsourcing to another laboratory – it did not need to maintain Personal Information about those consumers in order to conduct its business. CX0740 (Hill) ¶ 80.

4. LabMD Did Not Adequately Train Employees to Safeguard Personal Information

LabMD did not adequately train its employees to safeguard Personal Information or provide appropriate opportunities for its IT employees to receive security-related training about evolving threats. CX0740 (Hill) ¶ 91. Proper training is integral to a defense in depth strategy. A company should provide its employees with training regarding security mechanisms, acceptable use of computer equipment, current threats, and best practices. CX0740 (Hill) ¶¶ 87,

---

[100] CX0754 (LabMD's Supp. Resp. to First Set of Complaint Counsel's Interrogs. to Resp't) Interrog. 2.

[101] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers); CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 185-90, 192-94, 198-99 (LabMD performed no tests for 20-25% of consumers on whom it received and maintains personal information, and other labs performed tests on 20-25% of patients for whom LabMD did not perform tests). Based on these data, LabMD maintains the personal information of no fewer than 100,000 consumers for whom it performed no lab test. *See also* CX0718 (Hudson Dep. Tr.) at 23-24; 52-54, 59-62 (testifying that, beginning in January 2005, it was LabMD's practice to transfer every patient's information to the company, regardless of whether LabMD performed a test for the patient); CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 43-45, 80 (testifying that the name, date of birth, address, Social Security number, billing and insurance information of all Southeast Urology Network patients was sent to LabMD, regardless of whether LabMD performed tests for the patients).

88. A company should also provide its IT employees with periodic training on protecting against evolving threats. CX0740 (Hill) ¶ 89.

LabMD did not provide its non-IT employees with any training regarding security mechanisms or the consequences of reconfiguring security settings in applications. CX0740 (Hill) ¶ 90; CX0705; CX0706; CX0711; CX0714; CX0718; CX0719; CX0724; CX0734; CX0735.[102] Many LabMD employees could change security settings on their computers because they were given administrative rights over their workstations. CX0717; CX0735; CX0724; CX0705.[103] Likewise, LabMD did not provide its IT employees with formal security-related training regarding evolving threats. CX0740 (Hill) ¶ 91; CX0705; CX0707; CX0711; CX0717; CX0719; CX0734; CX0735.[104] LabMD's security practices were, as a result, reactive, incomplete, *ad hoc*, and ineffective. Among other consequences of LabMD's inadequate training detailed in the report of Professor Hill:

- Penetration testing was never done before May 2010;[105]

[102] CX0705 (Bradley Dep. Tr.) at 145-47; CX0706 (Brown Dep. Tr.) at 90-93; CX0711 (Dooley Dep. Tr.) at 148; CX0714 (Former LabMD Employee Dep. Tr.) at 85-87; 96-97; CX0718 (Hudson Dep. Tr.) at 52-54, 73; CX0719 (Hyer Dep. Tr.) at 160-62; CX0724 (Maire Dep. Tr.) at 32; CX0734 (Simmons Invest. Hrg. Tr.) at 61-62; CX0735 (Kaloustian Invest. Hrg. Tr.) at 128-30, 214-15.

[103] CX0717 (Howard Dep. Tr.) at 19-20 (stating that prior to sometime in 2005, all employees used the same administrator credentials); CX0735 (Kaloustian Invest. Hrg. Tr.) at 166-70, 189 (stating that all employees had administrative rights over their workstations, both desktop and laptop, regardless of job roles or titles); CX0724 (Maire Dep. Tr.) at 60-61, 80, 116-17 (stating that until October 2007, all LabMD employees had administrative rights to their computers); CX0705 (Bradley Dep. Tr.) at 147-49 (stating that all IT employees and department managers, as well as one or two other users, had administrative rights).

[104] CX0705 (Bradley Dep. Tr.) at 152; CX0707 (Bureau Dep. Tr.) at 38; CX0711 (Dooley Dep. Tr.) at 148-49; CX0717 (Howard Dep. Tr.) at 23, 26; CX0719 (Hyer Dep. Tr.) at 130, 160-62; CX0734 (Simmons Invest. Hrg. Tr.) at 60-62; CX0735 (Kaloustian Invest. Hrg. Tr.) at 208-09.

[105] Section IV.B.2, *supra*.

- Software with known flaws was not updated on servers that contained Personal Information;[106]
- Firewalls were disabled on servers that contained Personal Information;[107]
- Servers executed software that was no longer supported by vendors, including operating system and antivirus software;[108]
- There was no uniform policy requiring strong passwords or expiration of passwords;[109]
- Personal Information was transmitted and stored in an unencrypted format;[110]
- At least some employees were given administrative access accounts and were able to download and install software without restriction.[111]

CX0740 (Hill) ¶ 91.

5. LabMD Did Not Require Employees to Use Authentication-Related Security Measures

LabMD did not require its employees or other users with remote access to its network to use common, effective, authentication-related security measures. As part of a defense in depth strategy, companies should use strong authentication mechanisms to control access to workstations. CX0740 (Hill) ¶ 94. For example, usernames and passwords are a common authentication mechanism. However, their effectiveness depends on: (1) the strength of the passwords; and (2) how the passwords are stored and managed. CX0740 (Hill) ¶ 94. To

[106] Section IV.B.6, *infra*.

[107] CX0735 (Kaloustian Invest. Hrg. Tr.) at 92, 293-94.

[108] Section IV.B.6, *infra*.

[109] Section IV.B.5, *infra*.

[110] Section IV.B.2, *supra* (no email encryption); *see also* CX0725 (Martin Dep. Tr.) at 36; CX0734 (Simmons Invest. Hrg. Tr.) at 43-46; CX0735 (Kaloustian Invest. Hrg. Tr.) at 62-64, 302-04.

promote the effectiveness of usernames/passwords, a company should have policies that impose minimum requirements for passwords (e.g., length, required characters, change intervals) to ensure that they are strong. CX0740 (Hill) ¶ 94. To enforce these policies, a company's password management should be centralized, passwords should not be stored in clear text, and a cryptographic hash should be applied to the password before it is stored. CX0740 (Hill) ¶ 94.

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. CX0740 (Hill) ¶ 95; CX0311; CX0705; CX0707; CX0715; CX0718; CX0719; CX0727; CX0728; CX0733; CX0734; CX0735.[112] For example, LabMD employee Sandra Brown testified that she used the same username, sbrown, and password, labmd, to access her LabMD computer on site and remotely from 2006 to 2013. CX0740 (Hill) ¶ 95; CX0706.[113] Similarly, LabMD routinely created weak passwords for the user accounts it created for computers that it placed in its physician clients' offices. CX0740 (Hill) ¶ 95; CX0718; CX0728; CX0734.[114] Between at least October 2006 and June 2009, LabMD employees shared passwords that were used to access Personal Information. CX0740 (Hill) ¶ 95; CX0719;

---

[111] CX0715 (Gilbreth Dep. Tr.) at 64-65; CX0719 (Hyer Dep. Tr.) at 26-30; CX0724 (Maire Dep. Tr.) at 60-61, 63, 80, 116-17; CX0734 (Simmons Invest. Hrg. Tr.) at 37-39; CX0735 (Kaloustian Invest. Hrg. Tr.) at 167-72.

[112] CX0006 (LabMD Policy Manual) at 14; CX0311 (Email J. Boyle to M. Daugherty Subject: Fw: New domain login, attaching New domain login msg); CX0705 (Bradley Dep. Tr.) at 7, 128-30; CX0707 (Bureau Dep. Tr.) at 82-83; CX0715 (Gilbreth Dep. Tr.) at 67; CX0718 (Hudson Dep. Tr.) at 85-88; CX0719 (Hyer Dep. Tr.) at 26-27; CX0727 (Parr Dep. Tr.) at 102-03, 111-12; CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 39-41; CX0733 (Boyle Invest. Hrg. Tr.) at 181-84; CX0734 (Simmons Invest. Hrg. Tr.) at 153-57; CX0735 (Kaloustian Invest. Hrg. Tr.) at 34-36, 254-58.

[113] CX0706 (Brown Dep. Tr.) at 13.

CX0735.[115] Although LabMD used Microsoft Windows operating systems that included a functionality that could manage passwords centrally, LabMD did not use that functionality. CX0740 (Hill) ¶ 95; CX0705; CX0719; CX0735.[116] Finally, LabMD did not use two-factor authentication, which could have compensated for LabMD's failure to require the use of strong passwords. CX0740 (Hill) ¶ 95; CX0707; CX0734; CX0735.[117]

6. LabMD Did Not Maintain and Update Operating Systems and Other Devices

LabMD did not adequately maintain or update its operating systems of computers and other devices on its network. CX0740 (Hill) ¶ 100. Bugs are endemic to complex software, and attackers exploit software bugs to gain unauthorized access to consumers' Personal Information. CX0740 (Hill) ¶¶ 98, 99. Maintaining and updating operating systems of computers and other devices to protect against known vulnerabilities is integral to a company's defense in depth strategy. CX0740 (Hill) ¶ 99.

LabMD, however, did not adequately maintain or update its operating systems and other devices. For example, LabMD's servers used software with known vulnerabilities long after security professionals had identified those vulnerabilities. CX0740 (Hill) ¶ 100; CX0070;

---

[114] CX0718 (Hudson Dep. Tr.) at 85-88; CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 39-41; CX0734 (Simmons Invest. Hrg. Tr.) at 151-52.

[115] CX0719 (Hyer Dep. Tr.) at 26-27, 45, 74-75; CX0735 (Kaloustian Invest. Hrg. Tr.) at 79, 295.

[116] CX0705 (Bradley Dep. Tr.) at 7, 128-30 (when Bradley started in 2010 LabMD did not use domain controller to centrally manage passwords); CX0719 (Hyer Dep. Tr.) at 83-87 (password policy not enforced when Hyer started in 2009); CX0735 (Kaloustian Invest. Hrg. Tr.) at 167-72 (LabMD did not implement active directory).

[117] CX0707 (Bureau Dep. Tr.) at 83-84; CX0734 (Simmons Invest. Hrg. Tr.) at 47-48, 144, 156; CX0735 (Kaloustian Invest. Hrg. Tr.) at 257-58.

CX0717; CX0711.[118] Similarly, LabMD's servers were running the Windows NT 4.0 operating system in 2006 (CX0735[119]), *two years* after Microsoft recommended that customers migrate their servers to "'more secure Microsoft Operating system products as soon as possible.'" CX0740 (Hill) ¶ 100. Finally, a critical LabMD server used software that was configured with the default administrative password and had a "buffer overflow" vulnerability, both of which an attacker could have exploited. CX0740 (Hill) ¶ 100(d); CX0067; CX0724; CX0735.[120]

7. LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information

LabMD did not employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. CX0740 (Hill) ¶ 105. Because security threats evolve, a defense in depth strategy should include mechanisms to prevent the exploitation of vulnerabilities by an attacker and to detect unauthorized access. CX0740 (Hill) ¶ 103. For example, a company should not allow its employees to install software on computer workstations; should isolate backups of Personal Information from multi-purpose employee

[118] CX0070 (ProviDyn External Vulnerability Scan, May 19, 2010) at 1, 19, 37 (identifying as an "Urgent Risk" an anonymous login vulnerability on its FTP server, for which a solution had been published in 1999, concluding that "Overall Security Posture" of the server was "Poor"); CX0717 (Howard Dep. Tr.) at 34-37 (LabMD used FTP to receive Personal Information from its physician clients); CX0711 (Dooley Dep. Tr.) at 131-33 (LabMD used FTP to receive Personal Information from its physician clients).

[119] CX0735 (Kaloustian Invest. Hrg. Tr.) at 271-74.

[120] CX0067 (ProviDyn Network Security Scan - LabNet) at 22-23, 65 (identifying as an "Urgent Risk" a password vulnerability on LabMD's backup application, for which warnings had been published in 2005; identifying as a "Critical Risk" a buffer overflow vulnerability in the same application, for which warnings had been published in 2007; and concluding that the "Overall Security Posture" of the server was "Poor"); CX0724 (Maire Dep. Tr.) at 22-23 (identifying Veritas as LabMD's backup application); CX0735 (Kaloustian Invest. Hrg. Tr.) at 285-87 (describing backup processes).

workstations; and could use File Integrity Monitors to identify potential malicious activity. CX0740 (Hill) ¶ 104.

LabMD, however, did not engage in these or other practices to prevent or detect unauthorized access to Personal Information on its computer network. CX0735; CX0730; CX0719.[121] LabMD's policies did not prevent, detect, or remove the file-sharing application, LimeWire, for years after it was installed on the LabMD billing manager's workstation. CX0740 (Hill) ¶¶ 61, 105; CX0730; CX0735; CX0711; CX0443.[122] File Integrity Monitoring, which LabMD did not use, could have detected the application. CX0740 (Hill) ¶ 105; CX0734; CX0735.[123] In addition, LabMD actively stored backups of highly sensitive Personal Information on an employee's workstation. CX0710; CX0730.[124]

C. LabMD Did Not Correct Its Security Failures Despite the Availability of Free and Low-Cost Measures

Respondent could have corrected the security failures described above at relatively low cost, using readily available security measures. Professor Hill set forth free or low cost solutions

[121] CX0735 (Kaloustian Invest. Hrg. Tr.) at 90-93 (no process for risk assessment), 166-67 (administrative privileges), 173-175 (no automated scanning of desktops); CX0730 (Simmons Dep. Tr.) at 23-26, 38-39, 52-56 (no controls prevented employees from downloading file-sharing software to their computers); CX0719 (Hyer Dep. Tr.) at 37-38 (login credentials not revoked for former clients).

[122] CX0730 (Simmons Dep. Tr.) at 24-25, 54-56 (LimeWire installed on billing manager's computer in 2005 or 2006; LabMD did not use tools that could have detected the installation of a P2P application); CX0735 (Kaloustian Invest. Hrg. Tr.) at 269-70 (LabMD did not use tools that could have prevented or detected the installation of a P2P application); CX0711 (Dooley Dep. Tr.) at 117-19 (LabMD did not effectively prohibit or have the capability to detect the installation of a file-sharing application); CX0443 (Verified Resp. to Access Letter, Feb. 24, 2010) at 13 (Tiversa notified LabMD in May 2008 that it had downloaded the 1718 File).

[123] CX0734 (Simmons Invest. Hrg. Tr.) at 68-69 (LabMD did not use File Integrity Monitoring); CX0735 (Kaloustian Invest. Hrg. Tr.) at 92-93 (LabMD did not use File Integrity Monitoring).

[124] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 200 (1718 File stored on billing manager's computer); CX0730 (Simmons Dep. Tr.) at 22-26, 38-39 (1718 File was stored on billing manager's computer).

to LabMD's security failures in her report.

1. Comprehensive Information Security Program

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). These resources provided guidelines for creating a comprehensive security program to ensure the confidentiality, integrity, and availability of data and cover topics such as authenticating users, employing access control mechanisms to limit 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. CX0740 (Hill) ¶ 60.[125]

2. Identify Security Risks and Vulnerabilities

Professor Hill described several methods for identifying security risks and vulnerabilities, including the use of antivirus software, firewalls, and penetration testing. For each of these methods, she identified free or low cost solutions. For example, the firewall LabMD used until 2010 had limited risk assessment capabilities, and could not monitor traffic. Traffic monitoring allows an IT professional to determine if, for example, sensitive consumer information is being exported from a network. LabMD could have used a free program to analyze information traffic

[125] *See also* sources cited in CX0740 (Hill) ¶ 60 n.8; Section IV.A, *supra*.

leaving its network to determine if Personal Information was being exported. CX0740 (Hill) ¶ 68(b). Similarly, since 1997, free products have enabled companies to conduct their own penetration testing and network analysis. CX0740 (Hill) ¶ 71.[126] When LabMD hired an outside provider, ProviDyn, to conduct a penetration test in 2010, the cost was a modest $450. CX0044; CX0048; CX0488.[127] Those products could have helped the company to identify vulnerabilities such as outdated software, security patches that had not been applied, and administrative accounts with default settings. 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. CX0740 (Hill) ¶ 70.

3. Access Controls for Personal Information

LabMD could have restricted employee access to only to the Personal Information needed to perform their assigned job functions at relatively low cost. As Professor Hill explained, operating systems (such as Windows) and software applications offer role-based access control mechanisms as standard features. Implementing these features would not have required acquisition of additional hardware or software, only time from LabMD's IT staff. CX0740 (Hill) ¶ 85.

[126] Free penetration test tools included nmap (www.nmap.org, released 1997), Nessus (free until 2008), and Wireshark (formerly Etheral, released 1998).

[127] CX0044 (ProviDyn Service Solutions Proposal for LabMD, executed by M. Daugherty) at 4; CX0048 (ProviDyn invoice); CX0488 (ProviDyn 2010 Signed Service Solutions Proposal) at 4.

4. Training Employees to Safeguard Personal Information

Like implementing the access controls included in programs LabMD was already using, providing employee training on safeguarding information would have required only the expenditure of time by LabMD staff. LabMD provided staff with training on other topics. CX0718.[128] Nationally recognized organizations provide low-cost and free IT security training courses. CX0740 (Hill) ¶ 89.[129] With this training, IT staff could have provided training to all staff on safeguarding Personal Information.

5. Authentication-Related Security Measures

As with the access controls and training, creating password policies requires only the resource of time. The Windows operating system that LabMD used had as an included feature a centralized password management scheme. CX0740 (Hill) ¶ 95(a). Using this included feature would not have imposed additional cost.

6. Maintain and Update Operating Systems and Other Devices

When a provider sells an operating system or other software, it provides support in the form of patches and other fixes for bugs and security vulnerabilities. Such support is generally provided to users at no additional cost. CX0740 (Hill) ¶ 99. In addition to the vendors, other organizations such as CERT, OSVDB, and NIST provide free product notification systems to

[128] CX0718 (Hudson Dep. Tr.) at 48-49 (sales training).

[129] Professor Hill provided the following examples: "[T]he Center for Information Security Awareness, formed in 2007, provides free security training for individuals and businesses with less than 25 employees. The SysAdmin Audit Network Security Institute (SANS) formed in 1989, provides free security training webcasts. Additional free training resources may be found at http://msisac.cisecurity.org/resources/videos/free-training.cfm. The Computer

send alerts to IT practitioners about needed updates. CX0740 (Hill) ¶ 99. LabMD could have used these free vendor solutions to upgrade products and avoid security vulnerabilities. For example, fixes for vulnerabilities of the Veritas Backup software that were detected by penetration testing that LabMD conducted in 2010 had been made available in 2005 (stop use of default administrative password) and 2007 (fix vulnerability to a buffer overflow attack). CX0740 (Hill) ¶ 100(d); CX0737 (Hill Reb.) ¶ 19.

7. Prevent or Detect Unauthorized Access to Personal Information

Professor Hill identified a number of mechanisms to implement a defense-in-depth strategy to prevent or detect unauthorized access to Personal Information. CX0740 (Hill) ¶ 104. Implementing these methods would have been free or low cost. For instance, the Windows operating system used by LabMD allowed for, as standard features, giving employees non-administrative accounts on workstations to prevent them from installing software and implementing software firewalls on employee workstations. CX0740 (Hill) ¶¶ 104(a), (f). Storing backups of Personal Information on devices isolated from other employee activities could be cost-free, if an existing device is designated for storage purposes only. CX0740 (Hill) ¶ 104(b). Properly configuring existing firewalls does not add any additional cost. CX0740 (Hill) ¶¶ 104(e), (g), 105(c). Finally, Professor Hill recommended the use of a File Integrity Monitor to take snapshots of the systems and compare later snapshots to earlier ones to ensure

---

Emergency Response Team (CERT) at Carnegie Mellon University has e-learning courses for IT professionals for as low as $850." CX0740 (Hill) ¶ 89 n.30.

nothing has changed in the system. CX0740 (Hill) ¶ 104(h). Free versions are available. CX0740 (Hill) ¶ 104(h).

D. Security Incidents

1. LimeWire Installation and Sharing of 1718 File

In May 2008, a third party, Tiversa, Inc. ("Tiversa"), informed Respondent that LabMD's June 2007 Insurance Aging Report ("1718 File") was available on a P2P network. Ans. ¶ 17; CX0766; CX0025.[130] Tiversa, a company that offers breach detection and remediation services, contacted LabMD after having found the 1718 File. CX0703.[131] [redacted]

Tiversa informed LabMD that the 1718 File was available to other P2P users through the P2P file sharing application LimeWire, and that Tiversa was able to download the file. Ans. ¶ 18; CX0025; CX0703.[133] [redacted]

[130] Ans. ¶ 17 (Respondent admits that Tiversa "contacted LabMD in May 2008 and claimed to have obtained a June 2007 insurance aging report from LabMD via Limewire [sic], a P2P file sharing application."); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 39; [redacted] The June 2007 Insurance Aging Report ("1718 File") is 1,718 pages long (CX0008) and contains Personal Information for approximately 9,300 consumers (Ans. ¶ 19).

[131] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 10-11, 77-78.

[132] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 25, 77-78.

[133] Ans. ¶ 18 (Respondent admits that "Tiversa claimed that the 'P2P insurance aging file' could be obtained via Limewire [sic] in May 2008."); [redacted] CX0703 (Tiversa Depo. Tr.) at 36.

[redacted] Tiversa offered LabMD its remediation services in its initial telephone call to LabMD informing Respondent about the availability of its file on the P2P network and in emails that followed. CX0023; CX0025; CX0026; CX0803.[135]

After being notified in May 2008 that the 1718 File was available through LimeWire, LabMD determined that LimeWire had been downloaded and installed on a computer used by LabMD's billing department manager (the "Billing Computer"). Ans. ¶ 18(a); CX0755; CX0447; CX0150; CX0730.[136] LabMD determined that the P2P application 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) after Tiversa notified LabMD that the 1718 file was available on a P2P network. CX0730.[137] LabMD further determined the LimeWire application had been installed on the Billing Computer no later than 2006. Ans. ¶ 18(c); CX0447; CX0150.[138] In addition, LabMD found LimeWire was running

---

[134] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admissions 39: [redacted]; CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 36.

[135] CX0023 (Email J. Boyle to R. Boback Subject: Re: follow-up); CX0025 (Email J. Boyle to R. Boback Subject: Re: Tiversa/LabMD); CX0026 (Email R. Boback to J. Boyle Subject RE: Tiversa/LabMD, attaching Standard Incident Resp. Case SOW.pdf); CX0803 (Email R. Boback to J. Boyle Subject: FW: LabMD).

[136] Ans. ¶ 18(a) (admitting that LabMD "believes that Limewire [sic] had been downloaded and installed on a computer used by LabMD's billing department manager"); CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) Interrog. 3; CX0023 (Email J. Boyle to R. Boback Subject: Re: follow-up) (email from LabMD to Tiversa acknowledging file transfer); CX0447 (LabMD Access Letter Response by Dana Rosenfeld) (discussing the installation of LimeWire on LabMD Billing Computer) at 6-7; CX0150 (Screenshot: C:\) (screenshot showing "Date Modified" for a LimeWire StubInstaller Application on the LabMD Billing Computer as Oct. 31, 2005); CX0730 (Simmons Dep. Tr.) at 10.

[137] CX0730 (Simmons Dep. Tr.) at 10.

[138] Ans. ¶ 18(c) (Respondent admits that "it believes that a version of Limewire [sic] may have been installed on the billing computer no later than 2006."); CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6; CX0150

updates to the P2P application on the Billing Computer as late as April 25, 2008. CX0447.[139] LabMD admits that it removed LimeWire from the Billing Computer in May 2008, after receiving notice about the 1718 File's availability on a P2P network. Ans. ¶ 20. LabMD further admits to having had no business need for LimeWire on the Billing Computer. Ans. ¶ 20.

LabMD found that the 1718 File was maintained on the Billing Computer on which LimeWire had been installed. CX 0766.[140] The 1718 File contains Personal Information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers. Ans. ¶ 19; CX0766.[141] LabMD admits that the information of approximately 9,300 physician clients' "patients" were in the 1718 File, and for the purposes of the FTC Act, those individuals LabMD refers to as "patients" are consumers. Ans. ¶ 19; CX0766; *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 938-41 (N.D. Ill. 2008) (holding that, for the purposes of the FTC Act, the term "consumers" is defined broadly and "carries its ordinary or common meaning.").[142]

(Screenshot: C:\) (screenshot showing "Date Modified" for a LimeWire StubInstaller Application on the LabMD Billing Computer as Oct. 31, 2005).

[139] CX0447 (LabMD Access Letter Response by Dana Rosenfeld) at 6.

[140] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 42.

[141] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 37.

[142] Ans. ¶ 19 (Respondent admits that "the P2P insurance aging file contain[s] personal information about approximately 9,300 referring physicians' patients, including names, dates of birth, Social Security numbers, CPT codes, and health insurance company names, addresses, and policy numbers."); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 37.

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. CX0154; CX0152; CX0730.[143] These files 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." Ans. ¶ 18(b); CX0152.[144] Such files could have been found by using search terms and could have been of interest to other LimeWire users, including potential identity thieves. CX0738 (Shields) ¶¶ 57-58. LabMD was able to determine the number of files being shared by the Billing Computer through its employee's inspection in response to the call from Tiversa. The LabMD employee, Ms. Alison Simmons, took screenshots of LimeWire on the Billing Computer before removing the program. CX0150; CX0151; CX0152; CX0154; CX0155; CX0730.[145] The warnings that the LimeWire application displayed for the user indicated the Billing Computer was sharing many files and sub-folders. CX0152; CX0154.[146]

[143] CX0154 (Screenshot: LimeWire: Get Started) (screenshot of billing manager's computer, showing it sharing 913 files on the P2P network); CX0152 (Screenshot: LimeWire: My Shared Files) (screenshot of billing manager's computer, showing it sharing 953 files on the P2P network); CX0730 (Simmons Dep. Tr.) at 12-13, 21-30.

[144] Ans. ¶ 18(b) (Respondent admits that hundreds of music files were found on the billing computer and could be shared using Limewire [sic]."); CX0152 (Screenshot: LimeWire: My Shared Files).

[145] 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); CX0730 (Simmons Dep. Tr.) at 21-43.

[146] The warnings included an orange warning bar that states, "You are sharing 953 files. You can control which files LimeWire shares. Configure Library [link]" (CX0152 (Screenshot: LimeWire: My Shared Files)) and a pop-up warning that states, "You are sharing many subfolders within your shared folder: C\Documents and Settings\RWoodson\MyDocuments. This indicates a potential security problem, so please review your "My Shared Files" to ensure you aren't sharing any sensitive files." (CX0154 (Screenshot: LimeWire Get Started)).

[redacted]

2. Sacramento Incident

In October 2012, the Sacramento California Police Department found more than 35 LabMD "Day Sheets" in the possession of individuals unrelated to LabMD's business who later pleaded no contest to state charges of identity theft. CX0720; CX0085; CX0087; CX0107; CX0108.[149] The Sacramento Police Department also found approximately ten copied checks made payable to LabMD in the possession of the same individuals. CX0088.[150]

Day Sheets are reports that are generated electronically by LabMD's billing application, Lytec, to ensure payment was received and posted. CX0715; CX0714.[151] Day Sheets and copied checks were stored in paper files at LabMD, and LabMD had no policy in place to destroy those paper files. CX0733; CX0710; CX0715; CX0714.[152] Some of the Day Sheets and copied checks

[147] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 9.

[148] CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 52, 58, 61-64.

[149] CX0720 (Jestes Dep. Tr.) at 17-20, 22-23, 28-29, 33-36, 43-44; CX0085 (LabMD Day Sheets and Copied Checks); CX0087 (LabMD Day Sheets); CX0107 (Sup. Ct. of Cal.: Erick Garcia Minute Order re Plea); CX0108 (Sup. Ct. of Cal.: Josie Martinez Maldanado Minute Order re Plea)

[150] CX0088 (LabMD Copied Checks).

[151] CX0715 (Gilbreth Dep. Tr.) at 42-43; CX0714 (Former LabMD Employee Dep. Tr.) at 58-60.

[152] CX0733 (Boyle Invest. Hrg. Tr.) at 33-39, 45-46; CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 60; CX0715 (Gilbreth Dep. Tr.) at 43-44, 50-51; CX0714 (Former LabMD Employee Dep. Tr.) at 58-60.

were scanned and saved to the LabMD computer networks as part of the company's archive project. CX0733.[153]

The Day Sheets contain Personal Information about at least 500 consumers, including names, Social Security numbers, and in some cases, diagnosis codes. CX0766; CX0087; CX0742 (Kam) at 21-22.[154] The consumers listed in the Day Sheets come from different states. CX0087; CX0407.[155] Many of these consumers were not included in the 1718 File, and some of the Day Sheets post-date the 1718 File. A number of the Social Security numbers in the Day Sheets are being, or have been, used by people with different names, which may indicate that the Social Security numbers have been used by identity thieves. CX0742 (Kam) at 7, 23; CX0451.[156]

Complaint Counsel attempted to take discovery from the identity thieves who possessed the LabMD Day Sheets and copied checks. Complaint Counsel attempted to serve a subpoena *ad testificandum* on Josie Maldonado, but failed. CX0720.[157] Complaint Counsel successfully served Erick Garcia a subpoena *ad testificandum*, but Mr. Garcia asserted his Fifth Amendment right and did not respond substantively to questions related to how he came to possess the

[153] CX0733 (Boyle Invest. Hrg. Tr.) at 45-49.

[154] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 38; CX0087 (LabMD Day Sheets).

[155] CX0087 (LabMD Day Sheets); CX0407 (Mail Merge List of Persons for LabMD Notification Letter) at 40-43.

[156] CX0451 (Sacramentoresults7.xlsx Native File).

[157] CX0720 (Jestes Dep. Tr.) at 45 (stating that Maldonado could not be located by Sacramento law enforcement).

LabMD Day Sheets and copied checks that were found in his possession and resulted in his plea. CX0335; CX0712.[158]

V. LABMD'S DATA SECURITY PRACTICES WERE UNFAIR AND VIOLATE SECTION 5

A. Unfairness Standard and Burden of Proof

As discussed more fully above, Section IV.A, *supra*, Congress has defined an unfair practice as one that "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Rule 3.43(a) states that "Counsel representing the Commission . . . shall have the burden of proof," except as to factual propositions put forward by another proponent, such as affirmative defenses. *See also* Administrative Procedure Act, 5 U.S.C. § 556(d). The standard of proof is preponderance of the evidence. *In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *133-35 (Aug. 5, 2009) (collecting cases).

B. Unfairness Standard as Applied to Facts

1. Caused or is Likely to Cause Substantial Injury to Consumers

Respondent's failure to employ reasonable and appropriate measures to protect consumers' sensitive Personal Information caused or is likely to cause substantial injury to consumers.

[158] CX0712 (Garcia Dep. Tr.) at 9-10, 24-25, 28-29.

As described above, LabMD collected and stored on its computer network highly sensitive information about consumers, including names and addresses, dates of birth, Social Security numbers, medical test codes, and health information. Section II.A.2, *supra*. As previously detailed, LabMD provided unreasonable security for this extremely sensitive information through a series of actions and omissions. Section IV, *supra*. These failures caused or are likely to cause substantial injury to the nearly 10,000 consumers whose Personal Information was disclosed in the 1718 File and the Sacramento Day Sheets and copied checks, as well as the over 750,000 consumers whose Personal Information is maintained on LabMD's computer networks.

LabMD's failures placed the 9,300 consumers whose Personal Information was shared on a P2P network, the approximately 600 consumers whose Personal Information is contained in the Sacramento Day Sheets and copied checks, and the over 750,000 consumers whose Personal Information is maintained on LabMD's computer networks at risk of injury or harm,[159] including identity theft[160] and medical identity theft.[161] Further, the exposure of consumers' sensitive information as a result of LabMD's data security practices places those consumers at risk of a wide range of other harms, such as reputational injury, embarrassment, and public disclosure of

[159] "Injury" and "harm" are used interchangeably for purposes of this analysis.

[160] Identity theft, sometimes also referred to as identity fraud, is the unauthorized use of another's personally identifiable information to achieve illicit gain. CX0741 (Van Dyke) at 3; CX0742 (Kam) at 10. *See also* CX0720 (Jestes Dep. Tr.) at 13.

[161] 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. CX0742 (Kam) at 11.

an individual's most personal health history. These are the types of harms that are cognizable under Section 5. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (complaint's statements that LabMD's data security practices caused or were likely to cause increased risks of "identity theft," "medical identity theft," and "disclosure of sensitive medical information" adequately allege unfairness); Comm'n Stmt. of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("Policy Statement on Unfairness"), reprinted in *In re Int'l Harvester Co.*, 104 F.T.C. 949, 1984 WL 565290 at *97 (1984) (stating that in addition to monetary harms, "[u]nwarranted health and safety risks may also support a finding of unfairness"); *cf. Doe v. City of New York*, 15 F.3d 264, 267 (2d. Cir. 1994) (constitutional right to privacy in medical information).

a. Substantial Consumer Injury from Exposure of 1718 File

The exposure of the 1718 File places consumers whose sensitive Personal Information is in the file at risk of harm. Identity thieves frequently use the types of information in the file – including names, dates of birth, nine-digit Social Security numbers, and health insurance and billing information – to commit identity crimes. CX0741 (Van Dyke) at 12; CX0742 (Kam) at 18 (risk factors based on sensitivity of information); CX0720.[162] For instance, in combination with a consumer's name, Social Security numbers can be utilized to gain direct access to financial accounts. CX0741 (Van Dyke) at 5. Once a consumer's information is exposed, it is difficult for that consumer to detect and prevent misuse of his or her information. CX0742

[162] CX0720 (Jestes Dep. Tr.) at 14-15.

(Kam) at 8, 12; CX0721; CX0723.[163] Further, certain types of Personal Information, such as Social Security numbers, rarely change and thus can be used fraudulently for extended periods of time, placing consumers at risk of injury indefinitely. CX0741 (Van Dyke) at 5; CX0742 (Kam) at 22; CX0721.[164]

As described below, 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. CX0741 (Van Dyke) at 3; CX0742 (Kam) at 19; CX0721.[165]

i. **Identity Theft**

Consumers whose Personal Information was exposed in the 1718 File are at risk of suffering monetary harm from identity theft. Mr. Van Dyke projects that these consumers will experience financial harm from the disclosure of the 1718 File. CX0741 (Van Dyke) at 14. Drawing upon Javelin's identity fraud survey work, Mr. Van Dyke projects that consumers will incur [redacted] cases of existing card fraud,[166] existing non-card fraud,[167] and new account fraud[168] related to the

[163] CX0721 (Johnson Dep. Tr.) at 112-14; CX0723 (Lapides Dep. Tr.) at 47.

[164] CX0721 (Johnson Dep. Tr.) at 112.

[165] CX0721 (Johnson Dep. Tr.) at 108.

[166] Existing card fraud is identity theft perpetrated through the use of existing credit or debit cards and/or their account numbers. CX0741 (Van Dyke) at 3.

[167] Existing non-card fraud is identity theft 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) at 3.

exposure of the 1718 File. CX0741 (Van Dyke) at 8-14. Further, Mr. Van Dyke opines that consumers will spend [redacted] resolving fraud arising from the unauthorized disclosure of their sensitive information in the 1718 File. CX0741 (Van Dyke) at 14.

ii. Medical Identity Theft

The unauthorized disclosure of the 1718 File that resulted from LabMD's failures also caused or is likely to cause substantial injury to consumers in the form of medical identity theft. 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.

In his expert report and at the evidentiary hearing, Mr. Kam will testify that at least 76 consumers whose Personal Information is contained in the 1718 File are or are likely to be victims of medical identity theft. CX0742 (Kam) at 19. Of these 76 consumers, Mr. Kam estimates that no fewer than 27 are likely to incur an average out-of-pocket cost of $18,660. Mr. Kam notes that this 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) at 15. Mr. Kam estimates the likely total out-of-pocket cost to consumers from medical identity theft resulting from the unauthorized disclosure of the 1718 File to be in excess $500,000. CX0742 (Kam) at 20.

---

[168] New account fraud is a form of identity theft perpetrated through the use of another person's personally identifiable information to open new fraudulent accounts. CX0741 (Van Dyke) at 3.

In addition to suffering financial harm from medical identity theft, consumers whose Personal Information is in the 1718 File are also at risk of experiencing adverse health consequences. CX0742 (Kam) at 20; CX0741 (Van Dyke) at 13. For instance, Mr. Kam estimates that no fewer than 11 consumers will be misdiagnosed with the wrong illness, 11 consumers will experience a delay in medical treatment, 10 consumers will have an illness mistreated, 8 consumers will have the wrong pharmaceutical prescribed, and 30 consumers will lose their health insurance. CX0742 (Kam) at 20. Direct physical harm to the consumer could occur, for example, when a change is made to a consumer's medical record that could result in improper or unnecessary treatments. CX0741 (Van Dyke) at 13. When a consumer's electronic health record is compromised and the health information of the identity thief merges with that of the medical identity theft victim, the resulting inaccuracies could pose serious risks 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. CX0742 (Kam) at 15.

b. Consumer Injury from Exposure of Sacramento Day Sheets and Copied Checks

The exposure of the Sacramento Day Sheets and copied checks caused or is likely to cause substantial injury to consumers. The Day Sheets and copied checks contain sensitive Personal Information, including first names, last names, middle initials, and Social Security numbers for approximately 600 consumers, and bank routing and account numbers for consumers whose checks are included. CX0085.[169] Identity thieves value this type of Personal

[169] CX0085 (LabMD Day Sheets and Copied Checks).

Information and use it to commit identity theft resulting in monetary and other harms to the affected consumers. CX0741 (Van Dyke) at 5; CX0742 (Kam) at 22; CX0720.[170] Because consumers rarely change their Social Security numbers, these numbers can be fraudulently used for extended periods of time, placing consumers at heightened risk of injury. CX0741 (Van Dyke) at 5. The fact that the Day Sheets and copied checks were found, with other evidence of identity theft, in the possession of individuals who pleaded no contest to state charges of identity theft speaks to the value of the consumer information in the documents and the likelihood that it may have been misused. CX0742 (Kam) at 22-23; CX0720.[171]

Mr. Van Dyke estimates that consumers will incur [redacted] cases of existing card fraud, existing non-card fraud, and new account fraud related to the exposure of the Day Sheets. CX0741 (Van Dyke) at 12. Mr. Van Dyke also opines that consumers will spend over [redacted] resolving fraud arising from the unauthorized disclosure of their sensitive information in the Sacramento Day Sheets. Furthermore, Mr. Kam concluded that approximately 100 Social Security numbers in the Day Sheets appear to have been used by individuals with different names. CX0742 (Kam) at 23; CX0451.[172] The association of more than one name with the same Social Security number is an indicator of identity theft. CX0742 (Kam) at 23.

[170] CX0720 (Jestes Dep. Tr.) at 14-15.

[171] CX0720 (Jestes Dep. Tr.) at 33-35.

[172] CX0451 (Sacramentoresults7.xlsx Native File).

c. LabMD's Security Failures Placed All Consumers Whose Personal Information Is In Their Network at Risk.

LabMD's failure to employ reasonable and appropriate security measures puts at risk the Personal Information it maintains on its computer networks on hundreds of thousands of consumers. LabMD maintains Personal Information on over 750,000 consumers (CX0766[173]), including copies of hundreds of personal checks (CX0766[174]). This information includes: first and last name; address; date of birth; telephone number; Social Security number; medical record number; bank routing, account, and check numbers; credit or debit card information; laboratory test result, medical test code, diagnosis, or clinical history; and health insurance company name and policy number. Section II.A, *supra*.

Complaint Counsel's experts conclude that LabMD's failure to use reasonable and appropriate measures to prevent unauthorized access to sensitive Personal Information on its computer network creates an increased risk of disclosure of this information. CX0741 (Van Dyke) at 12-13; CX0742 (Kam) at 23; CX0740 (Hill) ¶ 49. This elevated risk, they note, is likely to cause substantial harm to consumers in the form of identity theft, medical identity theft, and other harms. CX0741 (Van Dyke) at 12-13; CX0742 (Kam) at 23.

d. Other Privacy Harms

[173] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers).

[174] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 32 (admitting that LabMD maintains paper copies of hundreds of personal checks from patients of its physician clients).

The exposure of the 1718 File also puts consumers at risk of experiencing other privacy harms. A prime example involves the current procedural terminology codes (CPT) in the file. Mr. Kam analyzed the codes, which indicate the diagnostic test(s) performed on a particular consumer, in the 1718 File. Upon reviewing the codes in the 1718 File, Mr. Kam discovered that many of the CPT codes relate to sensitive health conditions – for example, the presence of prostate cancer, testosterone levels, and sexually transmitted diseases, such as HIV, hepatitis, and herpes. CX0742 (Kam) at 21.

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) at 21. Moreover, once health information is disclosed, it is impossible to restore a consumer's privacy. CX0742 (Kam) at 21.

2. Harm Not Reasonably Avoidable by Consumers Themselves

Not only have LabMD's acts and omissions caused or are likely to cause substantial injury to consumers, but such injury is not reasonably avoidable by those consumers. As Mr. Kam states, "[a] consumer cannot know about the security practices of every company that collects or maintains his or her Personal Information." CX0742 (Kam) at 17. Record evidence from LabMD's physician clients demonstrates that consumers needing medical tests would not know which lab would test their specimen. CX0726; CX0728.[175] The consumers, therefore

[175] CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 78-79 (testifying that, except in limited circumstances, a patient would not know which lab was testing their specimen); CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 66-67 (testifying that great majority of patients did not know their specimen was going to LabMD).

have no knowledge of a lab's data security practices before their specimen was sent. CX0726; CX0728.[176] Consumers could not reasonably have avoided the harm caused by having their Personal Information provided to LabMD, which did not provide reasonable and appropriate security for that Personal Information.

3. LabMD's Failures Are Not Outweighed by Countervailing Benefits to Consumers or to Competition

LabMD could have avoided or remedied its unreasonable data security practices through readily available, low-cost measures. Section IV.C, *supra*. LabMD could have taken a host of free or low-cost measures, including but not limited to: (1) instituting a comprehensive information security program; (2) using an appropriate array of risk assessment methods, including conducting penetration tests; (3) restricting employees' access to Personal Information to only the types of Personal Information those employees needed to perform their jobs and purging data it collected from patients for whom it did not perform testing; (4) training employees to safeguard Personal Information; (5) requiring employees to use effective authentication-related security measures; (6) maintaining and updating operating systems and other devices; and (7) employing readily available measures to prevent or detect unauthorized access to Personal Information. Section IV.B, *supra*; CX0740 (Hill) ¶¶ 60, 69 n.22, 71, 77, 85, 92. Because there are few, if any, benefits to unreasonable data security practices, and LabMD's

[176] CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 78-79 (testifying that, except in limited circumstances, patient would not know about lab's data security practices before specimen was sent); CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 66-67 (testifying that great majority of patients would not know about LabMD's data security practices).

unreasonable security practices could have been remedied at little or no cost, there are no countervailing benefits to consumers or competition from LabMD's practices.

VI. RESPONDENT'S AFFIRMATIVE DEFENSES ARE UNAVAILING

A. First Affirmative Defense: Complaint Fails to State a Claim Upon Which Relief Can Be Granted

For its first affirmative defense, Respondent claims that "[t]he Complaint fails to state a claim upon which relief can be granted." In its order on Respondent's Motion to Dismiss, the Commission addressed Respondent's contention that "the Complaint does not state a plausible claim for relief," and that the allegations of the Complaint are legal conclusions rather than factual allegations. Comm'n Order Denying Resp't's Mot. to Dismiss at 17. The Commission ruled that this assertion is incorrect, and that the Complaint contains "plausible allegations that satisfy each element of the statutory standard for unfairness." *Id.* at 17-18. The Commission went on to consider the factual allegations supporting each element of unfairness, and concluded that the Complaint provides a plausible basis for each element. *Id.* at 18-19. The law of the case abrogates Respondent's first affirmative defense.

B. Second, Third, and Fifth Affirmative Defenses: Lack of Jurisdiction, Arbitrary and Capricious, Fair Notice

Respondent's Second, Third, and Fifth affirmative defenses claim that the Commission lacks jurisdiction or authority to bring data security enforcement actions for various reasons: that the Commission "is without subject-matter jurisdiction over the claims" (Second); that the Commission has no statutory authority to regulate the acts or practices in the Complaint and the

Commission's actions are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" (Third); and that the action "violates the due process requirements of fair notice and appropriate standards for enforcement guaranteed and protected by the Fifth Amendment to the U.S. Constitution and the Administrative Procedure Act" (Fifth).

The Commission has rejected the substance of Respondent's Second, Third, and Fifth Affirmative defenses, and thus the adequacy of the Commission's jurisdiction over and notice regarding data security standards is not before this Court for hearing. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 14-17 (holding that the Commission has "enforced Section 5's prohibition of 'unfair . . . acts or practices' primarily through case-by-case adjudication and litigation from the time the statute was enacted" and "the three-part statutory standard governing whether an act or practice is 'unfair' . . . should dispel LabMD's concern about whether the statutory prohibition of 'unfair . . . acts or practices' is sufficient to give fair notice of what conduct is prohibited"); *cf. FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019 at *14 (D.N.J. Apr. 7, 2014) (holding that "the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 'to the facts of particular cases arising out of unprecedented situations'" (citing *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965)).

C. Fourth Affirmative Defense: Respondent's Actions were Not Unfair

For its Fourth Affirmative Defense, Respondent claims that "[t]he acts or practices alleged in the Complaint do not cause, and are not likely to cause, substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by

countervailing benefits to consumers or to competition." This defense fails because, as described in Section V, *supra*, Respondent's acts or practices were and are unfair, in violation of Section 5. To the extent this affirmative defense echoes the Second, Third, and Fifth in its claim that "the Commission has no authority under Section 5 of the FTC Act to declare unlawful the acts or practices alleged in the Complaint," it is unavailing for the reasons stated in Section VI.B, *supra*.

VII. THE NOTICE ORDER SETS FORTH RELIEF APPROPRIATE FOR THIS CASE

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. at 394-95; *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," *In re Daniel Chapter One*, 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. National Lead Co.*, 352 U.S. 419, 428 (1957). As described in this brief, Respondent has acted in violation of the FTC Act as alleged in the Complaint, and the Notice Order is reasonably related to the alleged violations.

A. Specific Provisions of the Order

In addition to standard provisions relating to record-keeping, dissemination of the order to officers and employees, prior notification of corporate changes, filing compliance reports, and sunsetting, the notice order contains provisions specific to Respondent, tailored to the allegations

of the Complaint. Except for breach notice, *see* Section VII.A.3, *infra*, which will allow consumers to mitigate some harms resulting from Respondent's failures, these provisions do not impose costs beyond those that would be borne by any company implementing and maintaining reasonable security; as shown by the discussion in Section IV.C, *supra*, there are many low-cost or free solutions available to aid businesses in establishing and maintaining a comprehensive data security program.

1. Establish and Maintain a Comprehensive Data Security Program

The notice order requires that Respondent establish and maintain a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers" by Respondent or any entity owned or controlled by Respondent. The program must be in writing, and contain administrative, technical, and physical safeguards appropriate to Respondent's size and complexity, the nature and scope of its activities, and the sensitivity of the Personal Information. The notice order sets forth five criteria for a comprehensive information security program: (1) designation of an employee to coordinate and be accountable for the program; (2) identification of risks to Personal Information in specified areas; (3) design and implementation of reasonable safeguards; (4) development and use of reasonable steps to select service providers; and (5) evaluation and adjustment of the program in light of the results of tests and monitoring.

2. Obtain Initial and Biennial Assessments

The notice order further requires that Respondent obtain initial and biennial assessments

from a "qualified, objective, independent third-party professional." The assessment should: describe the safeguards Respondent has implemented and maintained; explain how the safeguards are appropriate to Respondent's size and complexity, nature and scope of its activities, and the sensitivity of Personal Information collected from consumers; explain how the safeguards meet the order provision relating to the establishment and maintenance of a comprehensive data security program; and certify that the Respondent's security program is operating effectively to provide reasonable assurance of the security of Personal Information.

3. Provide Notice to Affected Individuals

The notice order further provides that Respondent must provide notice to individuals whose Personal Information it has reason to believe was or could have been accessible to unauthorized persons, and that notice must contain: a brief description of why the notice is being sent, including the approximate time period of unauthorized disclosures and the types of Personal Information that may have been disclosed; advice on how individuals can protect themselves from identity theft, for which Respondent may refer individuals to FTC resources on identity theft; and the methods by which individuals can contact Respondent for further information. Respondent must make a reasonable effort to locate a mailing address for affected individuals. The notice order also requires that Respondent send a copy of the notice to each individual's health insurance company.

B. The Fencing-In Relief is Appropriate

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 *In re Telebrands*, 140 F.T.C. 278, 281 n.3 (2005)); *American 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. at 395; *Sears v. FTC*, 676 F.2d 385, 391-92 (9th Cir. 1982)). As several district courts have observed, "'[b]road injunctive provisions are often necessary to prevent transgressors from violating the law in a new guise.'" *FTC v. Nat'l Urological Group, Inc.*, 645 F. Supp. 2d 1167, 1215 (N.D. Ga. 2008) (quoting *FTC v. SlimAmerica, Inc.*, 77 F. Supp. 2d 1263, 1275 (S.D. Fla. 1999)), *aff'd*, 356 Fed. Appx. 358 (11th Cir. 2009)). An order must be "sufficiently clear that it is comprehensible to the violator," as well as "reasonably related" to the law violation. *Kraft*, 970 F.2d at 326 (internal quotation omitted).

The requirements that Respondent establish and maintain a comprehensive data security program and obtain initial and biennial assessments are standard in the FTC's data security orders. *See, e.g.*, cases cited in n.65, *supra*. In requiring the creation and implementation of a reasonable data security plan, these provisions are reasonably related to the Complaint's allegations that Respondent failed to maintain reasonable data security. Notice provisions are common not only in the FTC's data security orders, including orders relating to data security

requiring notice to consumers,[177] but also in orders in various other types of FTC cases in which third parties may have unwittingly participated in or been victimized by a respondent's conduct.[178] Where there is a likelihood of consumer harm, as here, such notice bears a reasonable relationship to the alleged violation as it informs consumers that they may be at risk of identity theft and other harms and provides them with information on how to avoid and mitigate the harm. Notice to the health insurance plans provides them a similar opportunity to protect consumers' identities from misuse. *Cf.* Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft ("Red Flags Rule"), 16 C.F.R. § 681.1 (requiring creditors, which can include medical providers, to "develop and implement a written Identity Theft Prevention

[177] *See, e.g.*, *United States v. InfoTrack Info. Svcs, Inc.*, No. 1:14-cv-02054 (N.D. Ill. Filed March 25, 2014) (consent order) (notice that consumer was included in a sex offender registry consumer report); *In re TRENDnet, Inc.*, FTC File No. 122-3090 (Sept. 4, 2013) (consent order) (notice of security flaw that may have allowed unauthorized users to view live feed of in-home cameras); *In re Compete, Inc.*, FTC Docket No. C-4384, FTC File No. 102-3155 (Feb. 20, 2013) (consent order) (notice that personal information may have been transmitted insecurely); *In re Upromise, Inc.*, FTC Docket No. C-4351, FTC File No. 102-3116 (Mar. 27, 2012) (consent order) (notice that personal information may have been transmitted insecurely). *See also In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *295 (Aug. 5, 2009).

[178] Third party notices may, for instance, be used to stop parties such as retailers from continuing to use deceptive claims in advertising. *See, e.g.*, *In re 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); *In re Oreck Corp.*, 151 F.T.C. 289, 371-72, 376-77 (May 19, 2011) (notice sent to franchisees); *In re 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); *In re Cytodyne LLC*, 140 F.T.C. 191, 209, 214-15 (Aug. 23, 2005) (notices sent to purchaser for resale of weight-loss supplement); *In re Snore Formula, Inc.*, 136 F.T.C. 214, 298-99, 304-05 (July 24, 2003) (notices sent to distributors who had purchased the product from the respondents or one of the respondents' other distributors); *In re MaxCell BioScience, Inc.*, 132 F.T.C. 1, 58-59, 66-67 (July 30, 2001) (consent) (notice to distributors); *In re Alternative Cigarettes, Inc.*, No. C-3956, 2000 FTC LEXIS 59, at *24, 31-33 (Apr. 27, 2000) (consent) (notices to retailers, distributors, or other purchasers for resale to which respondents supplied cigarettes); *In re Body Sys. Tech., Inc.*, 128 F.T.C. 299, 312, 318-19 (Sept. 7, 1999) (consent) (notice to distributors); *In re Brake Guard Prods., Inc.*, 125 F.T.C. 138, 259-60, 263-64 (Jan. 15, 1998) (notice to resellers); *In re Phaseout of Am., Inc.*, 123 F.T.C. 395, 457, 461-63 (Feb. 12, 1997) (notice to resellers); *In re Consumer Direct, Inc.*, No. 9236, 1990 FTC LEXIS 260, at *10-11, 20-21 (May 1, 1990) (notice to credit card syndicators); *In re Third Option Labs., Inc.*, 120 F.T.C. 973, 996, 1001 (Nov. 29, 1995) (notice to resellers); *In re Canandaigua Wine Co.*,

Program . . . that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account").

In analyzing whether there is a "reasonable relationship" between violations of the FTC Act and fencing-in provisions, courts consider "(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." *In re Daniel Chapter One*, 2009 FTC LEXIS 157, at *281 (citing *Telebrands*, 457 F.3d at 358; *Kraft*, 970 F.2d at 326). Applying these factors, the fencing-in relief in the notice order is appropriate.

1. Deliberateness and Seriousness of the Violation

As described in Section IV.B, *supra*, LabMD's approach to data security since at least 2005 was characterized by numerous failures that left the Personal Information of over 750,000 consumers vulnerable to misuse. LabMD's pattern and long history of unreasonable data security, as well as its failure to mitigate the dangers posed by unreasonable data security as described in Section IV.C, *supra*, show that Respondent acted deliberately. CX0719; CX0735; CX0734; CX0730; CX0724; CX0707.[179]

---

114 F.T.C. 349, 359-60 (June 26, 1991) (consent) (notice to distributors and retailers); *In re Removatron Int'l Corp*., 111 F.T.C. 206, 281, 319 (Nov. 4, 1988) (notice to device operators).

[179] CX0719 (Hyer Dep. Tr.) at 21-27 (detailing LabMD security failures observed on two-day visit, such as poorly enforced password policies, poorly enforced credential policies, and failure to implement administrative controls for software installation on computers); CX0735 (Kaloustian Invest. Hrg. Tr.) at 269-70 (stating that LabMD did not have capability to detect the installation or use of P2P software); CX0734 (Simmons Invest. Hrg. Tr.) at 160-61 (stating that LabMD did not have capability to detect the installation or use of P2P software); CX0730 (Simmons Dep. Tr.) at 53-56 (stating that LabMD did not have the capability to prevent installation of P2P software by some employees, and did not have the capability to detect installation or use of P2P software); CX0724 (Maire Dep. Tr.) at 94-95 (client computers not updated when more capable antivirus program purchased); CX0707 (Bureau Dep. Tr.) at 50-52 (computers not inspected unless employees reported a problem with them).

Respondent's unreasonable data security put over 750,000 consumers at risk of identity theft as well as a loss of their medical privacy and other harms, as discussed in Section V.B.1, *supra*. The seriousness of this danger is amply illustrated by the incidents related to the 1718 File and the documents recovered in Sacramento, in which the Personal Information of LabMD patients was obtained by third parties. *See* Section V.B.1, *supra*.

2. Degree of Transferability

In the advertising context, a violation is considered transferable when "other products could be sold utilizing similar techniques." *In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *284 (citing *Colgate-Palmolive*, 380 U.S. at 394-95; *Sears*, 676 F.2d at 392). Analogizing to the data security context, a violation is transferable when a company could obtain or continue to maintain consumers' Personal Information with unreasonable data security absent an order requiring the steps necessary to implement and maintain reasonable security. LabMD's violation of Section 5 of the FTC Act is transferrable for the following reasons: First, LabMD maintains Personal Information on over 750,000 consumers (CX0710; CX0765; CX0766[180]) on a network located in a private residence and a condominium. Section II.B, *supra*. This information includes the same types of sensitive information that were included in the 1718 File and in the Sacramento Day Sheets and copied checks. If Personal Information stored on LabMD's network were disclosed without authorization, it could be used to harm consumers.

[180] CX0710 (Daugherty, LabMD Designee, Dep. Tr.) at 60 (no policy of destroying paper day sheets), 215 (LabMD does not destroy records), 220-21 (data on Laboratory Information System cannot be destroyed); CX0765 (LabMD's Resps. to Second Set of Discovery) Interrogs. 12 and 17 (describing how personal information in Respondent's

Section V.B, *supra*. Second, LabMD has no intent to dissolve as a corporation. CX0765.[181] Instead, it is continuing to use the Personal Information it maintains to collect payments for services rendered (CX0709[182]) and to respond to requests from physicians (CX0291; CX0725.[183]). LabMD's collection activities will be conducted from a condominium using a workstation set up to access Personal Information stored on computers in LabMD's owner's private residence. CX0709; CX0727.[184] Third, the LabMD information technology employees who set up the network in the private residence and condominium have been dismissed, including the IT Manager (CX0709; CX0725[185]), apparently leaving no one to secure the network going forward (CX0725[186]). Finally, at the time the IT Manager was dismissed, no scans for vulnerabilities had been scheduled for the network, and Personal Information was not stored in an encrypted format and was secured only by a firewall. CX0725.[187]

In short, LabMD currently maintains Personal Information, and could obtain additional Personal Information of a similar level of sensitivity in the future. LabMD's data security practices affect all this information currently and in the future.

---

possession has been moved to a new location); CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 23 (admitting that LabMD maintains information on its network about more than 750,000 consumers).

[181] CX0765 (LabMD's Resps. to Second Set of Discovery) Interrogatory 11 ("LabMD does not intend to dissolve as a Georgia corporation.").

[182] CX0709 (Daugherty Dep. Tr.) at 19, 23-25.

[183] CX0291 (LabMD Letter to Physicians Offices re: Closing); CX0765 (LabMD's Resps. to Second Set of Discovery) Interrog. 10; CX0725 (Martin Dep. Tr.) at 19.

[184] CX0709 (Daugherty Dep. Tr.) at 28, 54-57; CX0727 (Parr Dep. Tr.) at 50.

[185] CX0709 (Daugherty Dep. Tr.) at 18; CX0725 (Martin Dep. Tr.) at 9, 24.

[186] CX0725 (Martin Dep. Tr.) at 114.

[187] CX0725 (Martin Dep. Tr.) at 113-14.

3. History of Violations

While the Commission has not previously brought a case against LabMD and does not allege prior violations of the FTC Act, the time period through which Respondent's conduct stretches indicates that fencing-in relief is appropriate. Furthermore, in the balancing test used to determine the appropriateness of order provisions, the presence of some strong factors can weigh in favor of fencing-in without the presence of other factors. *Telebrands*, 457 F.3d at 362; *In re Daniel Chapter One*, No. 9329, 2009 FTC LEXIS 157, at *284-85.

VIII. CONCLUSION

The evidence at the evidentiary hearing will show that Respondent violated Section 5 of the FTC Act by failing to protect consumers' Personal Information from unauthorized disclosure with reasonable and appropriate data security, that its actions caused or were likely to cause substantial consumer harm that consumers could not avoid, and that its failures were not outweighed by any benefit to consumers or competition. Accordingly, Complaint Counsel respectfully requests that this Court enter an appropriate order.

Dated: May 6, 2014

Respectfully submitted,

Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs
Jarad Brown

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2282 – Cox
Facsimile: (202) 326-3062
Electronic mail: mcox1@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on May 6, 2014, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system:

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

I also certify that I caused a copy of the foregoing document to be delivered *via* electronic mail and by hand 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* electronic mail to:

Michael Pepson
Lorinda Harris
Hallee Morgan
Robyn Burrows
Kent Huntington
Daniel Epstein
Patrick Massari
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org
lorinda.harris@causeofaction.org
hallee.morgan@causeofaction.org
robyn.burrows@causeofaction.org
kent.huntington@causeofaction.org
daniel.epstein@causeofaction.org
patrick.massari@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.

May 6, 2014 By: Megan Cox

Megan Cox
Federal Trade Commission
Bureau of Consumer Protection

Exhibit 1

Glossary

Antivirus: Software installed on a computer or network used to prevent and detect computer viruses and other malicious software. CX0740 (Hill) ¶¶ 31(e), 65.

Applications: Software that runs on a computer and receives data. Applications correspond to port numbers, and together, an application and its port(s) are the doors to computers and the networks to which the computers are connected. CX0740 (Hill) ¶ 19.

Authentication: The method employed by a computer or network user to tell the system who they are (identity) and prove they are who they say they are (proof). Usernames and passwords are commonly used to authenticate users. CX0740 (Hill) ¶ 25.

CERT: Computer Emergency Response Team at Carnegie Mellon University, an organization that provides free research and information on computer security. CX0740 (Hill) ¶ 89 n.30. For a list of relevant publications, see generally CX0740 (Hill) at Appendix B, "Web Content Considered or Relied Upon."

Defense in Depth: The practice of using a layered approach to security by implementing 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. CX0740 (Hill) ¶¶ 27-31, 52; CX0737 (Hill Reb.) ¶ 7.

File Integrity Monitor ("FIM"): Security software that takes an initial snapshot of the files that are stored on a computer and periodically monitors the system to determine whether any changes have occurred. Any change may indicate malicious activity and raises an alert notification. CX0740 (Hill) ¶ 104(h).

File Sharing Application: Software designed to share the music, videos, pictures, and other materials stored on a consumer's computer with other users. LimeWire is an example of a file sharing application. Ans. ¶ 13; CX0738 (Shields) ¶¶ 13, 14.

File Transfer Protocol ("FTP"): A protocol (*see* "Protocol," below) used to transfer files between computers on a network. CX0740 (Hill) ¶ 34.

Firewall: Hardware or software used to protect networks and individual computers from outside access. A firewall may operate by, for example, closing unused ports, or by limiting or preventing incoming connection requests to a network or computer. CX0740 (Hill) ¶¶ 21-22.

Gnutella Network: The Gnutella network consists of all computers running a file sharing program (such as LimeWire) to communicate online and participate in the Gnutella protocol. CX0738 (Shields) ¶¶ 15, 23-26.

Hash: A long number calculated from the data that makes up a particular file. A hash is statistically unique to that file. A hash may be used in P2P file sharing; a peer can compute the

hash of the requested file and compare it to the hash of a file obtained on the network and downloaded to the user's computer to ensure they are identical. CX0738 (Shields) ¶¶ 19, 28.

Host: A computer that provides some service(s) to other computers that are connected to it via a network. CX0054 (ProviDyn Network Security Scan - Mapper) at 38-39.

Insurance Aging Report: A report generated by LabMD's Lytec software showing outstanding payments due to LabMD by insurance companies. CX0706 (Brown Dep. Tr.) at 20-24; *see also* CX0715 (Gilbreth Dep. Tr.) at 7 (explaining that aging is accounts receivable).

Intrusion Detection System ("IDS"): A device placed inside a protected network to monitor activity in order to identify suspicious events. An IDS acts as a sensor, like a smoke detector, that raises an alarm if specific things occur. It may perform a variety of functions including: monitoring users and system activity; auditing system configuration for vulnerabilities and misconfiguration; assessing the integrity of critical system and data files; identifying known attack patterns in system activity; recognizing abnormal activity through statistical analysis; managing audit trails and highlighting user violations of policy; correcting system configuration errors; and installing and operating traps to record information. CX0740 (Hill) ¶ 23.

Laboratory Information System (LIS): *See* Labnet Server.

Labnet Server: The computer hosting the Laboratory Information System (LIS) that would import consumers' data from physicians' offices to LabMD's laboratory and billing applications, through the MAPPER server. CX0443 (Verified Resp. to Access Letter, Feb. 24, 2010) at 6; CX0725 (Martin Dep. Tr.) at 62-64, 67.

LabSoft: The laboratory application that LabMD ran on the Labnet server. CX0443 (Verified Resp. to Access Letter, Feb. 24, 2010) at 6; CX0735 (Kaloustian Invest. Hrg. Tr.) at 30-31, 50-51.

LimeWire: A file-sharing or peer-to-peer application that ran on the Gnutella network. CX0738 (Shields) ¶¶ 13-14.

Lytec: The billing application LabMD's billing department utilized in conjunction with the Labnet Server. CX0443 (Verified Resp. to Access Letter, Feb. 24, 2010) at 6; CX0733 (Boyle, LabMD Designee, Invest. Hrg. Tr.) at 40; CX0735 (Kaloustian Invest. Hrg. Tr.) at 54-55.

MAPPER Server: The server that received consumers' personal information and processed it to be used by LabMD's laboratory and billing applications. CX0740 (Hill) ¶ 35; CX0735 (Kaloustian Invest. Hrg. Tr.) at 51-55, 225; CX0725 (Martin Dep. Tr.) at 82-83.

Network: A group of computers, servers, and other devices that are connected by a communications channel that is either wired or wireless. CX0740 (Hill) ¶ 13. A Local Area Network (LAN) is an example of a network. CX0054 (ProviDyn Network Security Scan - Mapper) at 38.

NIST: The National Institute of Standards and Technologies, which publishes information on, *inter alia*, computer and network security. CX0740 (Hill) ¶¶ 60, 99. For a list of relevant publications, see generally CX0740 (Hill) at Appendix B, "Web Content Considered or Relied Upon."

OSVDB: Open Source Vulnerability Database, an organization that provides information on computer and network vulnerabilities. CX0740 (Hill) ¶ 99. For a list of relevant publications, see generally CX0740 (Hill) at Appendix B, "Web Content Considered or Relied Upon."

Patch: To apply updates to fix all known or reasonably foreseeable security vulnerabilities and flaws. CX0740 (Hill) ¶ 31(b).

Peer-to-Peer or P2P: The term "P2P" can apply to software (*see* "File-Sharing Application," above) or to the network created by the software. The network is comprised of computers that run P2P applications, called "peers" or "nodes." Each peer participates in the network, communicating over the Internet to provide and receive files such as music or documents. CX0738 (Shields) ¶¶ 13-15.

Penetration Testing: The term Penetration Testing," or "Pen Testing," refers to one type of probe that searches a network for security flaws. Penetration testing includes scanning ports to verify that unused ports are closed or disabled. CX0740 (Hill) ¶ 31(f).

Personal Information: As defined in the Notice Order, 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. Notice Order at 7.

Port: A computer's network interface is divided into several channels, each of which is called a "port." CX0054 (ProviDyn Network Security Scan - Mapper) at 39. Applications communicate via ports. There are well-known ports for well-known applications. For example, web servers typically use port number 80 to accept connections from users' web browsers. CX0740 (Hill) ¶¶ 19-20, 31(c).

Port Scan: The process of examining a group of ports on a computer to determine which ones are active. A port scan does not identify which applications/services are running on a computer, what any active ports are used for, or any security threats on the computer. It only determines which ports are active. CX0054 (ProviDyn Network Security Scan - Mapper) at 39.

Probe: Probing is a security audit that tests the state of a network. One type of probing is penetration testing, which searches the network for security flaws. CX0740 (Hill) ¶ 31(f).

Protocol: A standard procedure for regulating data transmission between computers. For example, an email server uses a specific set of protocols or rules so that anyone on the internet can send email to anyone else on the internet, regardless of the software or internet service provider either party is using. CX0054 (ProviDyn Network Security Scan - Mapper) at 39.

Risk Assessments: A term that refers to using readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its network. CX0740 (Hill) ¶ 63. *See also* CX 0400, at p. 55 ("The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.")

SANS: The SysAdmin Audit Network Security Institute, formed in 1989, provides free security training webcasts. CX0740 (Hill) ¶ 89 n.30. *See generally* CX0740 (Hill) at Appx. B, "Web Content Considered or Relied Upon."

Server: A computer that provides some service(s) to other computers that are connected to it via a network. For example, a web server provides web pages to a computer via the internet. CX0054 (ProviDyn Network Security Scan - Mapper) at 39.

Security Scan: The process of using various information security methodologies and techniques to audit the level of security for a computer, application, service, and/or network. CX0054 (ProviDyn Network Security Scan - Mapper) at 39.

Two-factor Authentication: An authentication mechanism (*see* "Authentication," above) that requires multiple forms of proof of identity to ensure the user is associated with a username. For example, after entering the username a user may be required to provide a password (what she knows) and also something she possesses, such as a biometric (finger print, iris scan, etc.). CX0740 (Hill) ¶ 25.

Veritas: An application used by LabMD to back up data. CX0740 (Hill) ¶ 100(d); CX0737 (Hill Reb.) ¶ 19; CX0067 (ProviDyn Network Security Scan – LabNet) at 8.

Exhibit 2

LabMD Employees

1. John Boyle, former LabMD Vice President of Operations.

Mr. Boyle worked at LabMD from November 1, 2006 to the end of August, 2013 as Vice President of Operations and General Manager. CX0704 (Boyle Dep. Tr.) at 6-8. Mr. Boyle oversaw the operations of the laboratory, IT, customer service, and billing. *Id.* at 9.

2. Brandon Bradley, former LabMD IT employee

Mr. Bradley worked at LabMD from approximately May 2010 to February 7, 2014. CX0705 (Bradley Dep. Tr.) at 7-8. While at LabMD, Mr. Bradley provided computer helpdesk services to LabMD employees and to Atlanta-area clients of LabMD. *Id.* at 9. Mr. Bradley was supervised by Jeff Martin, John Boyle, and Bob Hyer. *Id.*at 11-12.

3. Sandra Brown, former LabMD finance or billing employee

Ms. Brown was LabMD's billing manager from May 2005 to May 2006. CX0706 (Brown Dep. Tr.) at 6-7. During her tenure, the billing department billed patients and insurance, and engaged in correspondence and debt collection. *Id.* at 16. From May 2006 through March 2013, Ms. Brown worked for LabMD remotely from her home on insurance aging reports, using remote access software to enter LabMD's system. *Id.* at 6-7, 10-11. Insurance aging reports were used to collect outstanding payments due from insurance companies. *Id.* at 20; 140-41. In both capacities Ms. Brown was supervised by Michael Daugherty. *Id.* at 7. As Billing Manager, Ms. Brown worked with John Boyle and Tricia Gilbreth. *Id.*

4. Matt Bureau, former LabMD IT employee

Mr. Bureau worked for LabMD from December 2008 through April 2010. CX0707 (Bureau Dep. Tr.) at 7. Mr. Bureau was responsible for setting up new computers for LabMD's employees and customers. *Id.* at 8, 11, 12-13. At the beginning of his tenure, Mr. Bureau worked with Alison Simmons and Kurt Kaloustian. *Id*. at 7, 9-10. Mr. Bureau was supervised by John Boyle when he began working at LabMD, *id*. at 8, and was then supervised by Robert Hyer. *Id*. at 10.

5. Michael Daugherty, LabMD President and Chief Executive Officer

Michael Daugherty has been the President and Chief Executive Officer of LabMD from at least January 1, 2005 through the present. CX0709 (Daugherty Dep. Tr.) at 6-7.

6. Jeremy Dooley, former LabMD Communications Coordinator and IT employee

Mr. Dooley worked for LabMD from approximately October or November 2004 through December 2006. CX0711 (Dooley Dep. Tr.) at 12-13. Mr. Dooley began at LabMD doing insurance benefit verifications and then moved to receiving and sorting testing specimens. *Id.* at 13-14. Eventually Mr. Dooley began providing IT services, such as providing tech support to LabMD's clients and working on report formats. *Id.* at 14-18. After being named Communications Coordinator, Mr. Dooley became more heavily involved in IT. *Id.* at 36. His responsibilities including installing freeware antivirus onto remote-access computers and locating freeware remote access software. *Id*. at 72-75. Pat Howard was the IT manager during this time, *id*. at 18, and Mr. Dooley was supervised by Michael Daugherty. *Id*.

7. Kim Gardner, former LabMD Executive Assistant

Ms. Gardner worked at LabMD from November 2010 through December 2013. CX0713 (Gardner. Dep. Tr.) at 9-10. Ms. Gardner's title was Executive/Personal

Assistant, and she provided support to Michael Daugherty and John Boyle. *Id.* at 18. Ms. Gardner was involved in many functions at LabMD; her job responsibilities included human resources work, such as handing out and collecting new hire paperwork and handling benefits packages; mail handling; depositing patient and insurance payments; filing court documents; and stocking and maintaining the break room. *Id.* at 18-19. She also provided services to Michael Daugherty in his personal capacity, such as maintaining his rental condominiums and hiring construction workers to complete remodeling work on his residence. *Id.* at 18-19.

8. [redacted]

9. Patricia Gilbreth, former LabMD finance or billing employee

Ms. Gilbreth worked at LabMD from August 20, 2007 through December 30, 2013. CX0715 (Gilbreth Dep. Tr.) at 6. Ms. Gilbreth was the Finance Manager and Billing Manager. CX0733 (Boyle Invest. Hrg. Tr.) at 42-43; CX0715 (Gilbreth Dep. Tr.) at 8. As finance manager she 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 (Gilbreth Dep. Tr.) at 7. As billing manager, Ms. Gilbreth supervised the billing employees. CX0715 (Gilbreth Dep. Tr.) at 12-13.

10. Nicotra Harris, former LabMD finance or billing employee

Ms. Harris worked at LabMD from October 2006 through January 28, 2013. CX0716 (Harris Dep. Tr.) at 11. Ms Harris was a billing specialist; her initial responsibilities were billing, collections, and posting payment, and she progressed to posting all insurance and handling appeals and calls from doctors' offices. *Id.* at 11-12. Ms. Harris was supervised by Rosalind Woodson until Ms. Woodson left the company in August 2008, and then by Patricia Gilbreth. *Id.* at 13.

11. Patrick Howard, former LabMD IT employee

Mr. Howard worked for LabMD from March 2004 through March 2007. CX0717 (Howard Dep. Tr.) at 7. Mr. Howard was Director of IT. *Id.* at 8. Mr. Howard was responsible for running the LabSoft software, ensuring the servers were working, and managing network security. *Id.* at 10-11. Mr. Howard also set up servers and workstations for non-laboratory LabMD employees. *Id.* at 12-13. Mr. Howard was supervised by Michael Daugherty. *Id.* at 8-9.

12. Lawrence Hudson, former LabMD sales employee

Ms. Hudson worked for LabMD from approximately January or February 2004 through June or July 2007. CX0718 (Hudson Dep. Tr. at 14). Ms. Hudson was a territory manager. *Id.* at 14, 16. She worked in New Jersey, Pennsylvania, Tennessee, Kentucky, Alabama, Georgia, Mississippi, Louisiana, Arkansas, and Florida to secure new urology practice clients for LabMD, as well as to train sales representatives and develop marketing materials. *Id.* at 15-17. She served as the "face" of LabMD for

urology clients. *Id.* at 25. Ms. Hudson initially reported to Michael Daugherty, and then to the national sales manager. *Id.* at 25-26.

13. Robert Hyer, former LabMD IT Manager and former LabMD contractor

Mr. Hyer started his work at LabMD as a two-day consultation on data security in June 2009 (CX0719 (Hyer Dep. Tr.) at 15-16, 30-31), which resulted in a two month contract. *Id.* at 16. Upon expiration of the contract in August 2009, Mr. Hyer joined LabMD full time as Director of IT. *Id.* at 49. He left in March 2012. *Id.* at 47. Mr. Hyer was in charge of network security. CX0704 (Boyle Dep. Tr.) at 12. Mr. Hyer was supervised by John Boyle. CX0714 (Hyer Dep. Tr.) at 50.

14. Curt Kaloustian, former LabMD IT employee

Mr. Kaloustian worked for LabMD from October 2006 (CX0735 (Kaloustian Invest. Hrg. Tr.) at 17), until approximately April or May 2009. *Id.* at 7. He began at LabMD as IT support person and eventually became the primary IT resource for the company, *id.* at 14, as the unofficial "Lead IT Analyst." *Id.* at 18. He maintained the network architecture, maintained the servers, applied patches and implemented upgrades, built client interfaces, ensured data hygiene, and managed employee desktops. *Id.* at 14-15. Mr. Kaloustian was in charge of network security. CX0707 (Bureau Dep. Tr.) at 12; CX0724 (Maire Dep. Tr.) at 12. Mr. Kaloustian was initially supervised by Michael Daugherty, and then by John Boyle. CX0735 (Kaloustian Invest. Hrg. Tr.) at 16-17.

15. Eric Knox, former LabMD sales employee

Mr. Knox worked for LabMD from February 2005 through May 2007. CX0722 (Knox Dep. Tr.) at 15. Mr. Knox was a sales representative; his job was to secure new urology practice clients for LabMD. *Id.* at 16-17. He served as the "face" of LabMD for urology clients. *Id.* at 17. Mr. Knox's territory included Texas, Oklahoma, Arkansas,

and Louisiana. *Id.* at 19. Mr. Knox initially reported to Michael Daugherty, and then to a sales manager. *Id.* at 17.

16. Chris Maire, former LabMD IT employee

Mr. Maire worked for LabMD from approximately July 2007 through June or July of 2008. CX0724 (Maire Dep. Tr.) at 10, 37-38. He provided tech support, troubleshooting errors on employee workstations, prepping computer systems to be provided to LabMD clients, and repairing and maintaining peripherals such as printers. *Id*. at 10, 13-14. He participated in network security work, such as maintaining firewalls, when requested to do so, *id.* at 14, but did not have primary responsibility for network security. *Id.* at 12 (identifying Curt Kaloustian as responsible for network security). His work in the IT department was directed by John Boyle. *Id.* at 12.

17. Jeff Martin, former LabMD IT employee and former LabMD contractor

Mr. Martin started at LabMD on January 25, 2012, and was employed at the company at least through the date of his deposition, February 6, 2014. CX0725 (Martin Dep. Tr.) at 9. Mr. Martin served as IT Manager, and supervised two employees, Brandon Bradley and Jennifer Parr. *Id.* at 9-10. Mr. Martin was responsible for: querying the databases to retrieve, for instance, patient data; ensuring backups were run; and checking the security of the system. *Id.* at 27. Mr. Martin was in charge of network security. CX0704 (Boyle Dep. Tr.) at 12. Mr. Martin reported to John Boyle and Michael Daugherty. CX0725 (Martin Dep. Tr.) at 46.

18. Jennifer Parr, former LabMD IT employee

Ms. Parr worked for LabMD from May 2010 (CX0705 (Bradley Dep. Tr.) at 7-11) through February 2014 (CX0727 (Parr Dep. Tr.) at 16-17). Ms. Parr was LabMD's Systems Administrator. CX0727 (Parr Dep. Tr.) at 19. In that role she: ensured 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. *Id.* at 19-21. Ms. Parr reported directly to Robert Hyer, and indirectly to John Boyle. *Id.* at 36.

19. Alison Simmons, former LabMD IT employee

Ms. Simmons worked for MabMD from October 2006 through August 2009. CX0734 (Simmons Invest. Hrg. Tr.) at 14. Ms Simmons was an IT Specialist for the company. *Id.* Her responsibilities were to respond to phone calls from clients regarding the system; to manage the database and the data within it; to generate reports; to support the system connected LabMD and its clients; and to build and maintain computers for LabMD employees and clients. *Id.* at 14-15. Ms. Simmons' security responsibilities included ensuring that computers were protected by antivirus. *Id.* at 21. Ms. Simmons was supervised by John Boyle and Michael Daugherty. *Id.* at 53.

20. Rosalind Woodson, Former Billing Manager for LabMD.

Ms. Woodson worked for LabMD from June 1, 2006 through July 31, 2008. CX0681 (R. Woodson Dates of Employment) at 7. Ms. Woodson was the Billing Manager. CX0733 (Boyle Invest. Hrg. Tr.) at 27. LimeWire was downloaded and installed on Ms. Woodson's computer. Ans. ¶ 18(a); CX0755; CX0730.[1] LimeWire was sharing the 1,718 File and hundreds of other files from Ms. Woodson's computer. CX0766; CX0154; CX0152; CX0730.[2]

[1] Ans. ¶ 18(a) (admitting that LabMD "believes that Limewire [sic] had been downloaded and installed on a computer used by LabMD's billing department manager"); CX0755 (LabMD's Resp. to First Set of Interrogs. and Reqs. for Prod.) Interrog. 3; CX0730 (Simmons Dep. Tr.) at 10-11 (identifying Rosalind Woodson as the billing manager on whose computer LimeWire was installed).

[2] CX0766 (LabMD's Resps. and Objs. to Reqs. for Admission) Admission 42; CX0154 (Screenshot: LimeWire: Get Started) (screenshot of billing manager's computer, showing it sharing 913 files on the P2P network); CX0152 (Screenshot: LimeWire: My Shared Files) (screenshot of billing manager's computer, showing it sharing 953 files on the P2P network); CX0730 (Simmons Dep. Tr.) at 12-13, 21-30.

Current and Former Clients of LabMD

21. Letonya Randolph, Midtown Urology, PC ("Midtown Urology") employee, Midtown Urology designee

Midtown Urology is a Georgia practice that provides urological services to patients. CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 15-16. Since at least 2001, Midtown Urology has been a client of LabMD. *Id.* at 19. Midtown Urology transmitted patient information to LabMD electronically, using hardware provided by LabMD. *Id.* at 32, 47-48. Ms. Randolph is currently Midtown Urology's manager of medical assistants. *Id.* at 6

22. Barbara Goldsmith, Midtown Urology, PC ("Midtown Urology") employee

Ms. Goldsmith is Midtown Urology's practice manager. CX0728 (Randolph, Midtown Urology Designee, Dep. Tr.) at 44. Ms. Goldsmith signed Midtown Urology's Certification of Records of Regularly Conducted Activity. CX0289.

23. Jerry Maxey, Southeast Urology Network ("S.U.N.") employee, S.U.N. designee

S.U.N. is a urology practice with offices in Memphis and South Haven. CX0726 (Maxey, Southeast Urology Network Designee, Dep. Tr.) at 17. S.U.N. was a client of LabMD's from 2003 until approximately May 2012. *Id.* at 22, 83. LabMD provided S.U.N. with the hardware and software it used to transfer data to LabMD. *Id.* at 22-24, 27-28. Mr. Maxey is S.U.N.'s administrator. *Id.* at 5.

LabMD Contractors and Service Providers

24. Lou Carmichael, former LabMD consultant

Ms. Carmichael provided consulting services to LabMD from approximately 2001 or 2002 through 2009 or 2010. CX0708 (Carmichael Dep. Tr.) at 19-20. Ms. Carmichael was hired to create a compliance program, including training materials, and to provide

training on the compliance program. *Id.* at 19. Elements of the compliance program included fraud and abuse, self-referral, anti-kickback, and CLIA (Clinical Laboratory Improvement Act of 1988). *Id.* at 16 (describing compliance program for UroCor), 20 (stating LabMD compliance program very similar to UroCor compliance program). Ms. Carmichael's training program included some information on the use of personal information, but did not cover IT information security practices. *Id.* at 25-26. Ms. Carmichael reported to Michael Daugherty. *Id.* at 20.

25. Hamish Davidson, President of ProviDyn, Inc.

Mr. Davidson is the President of ProviDyn, Inc., a company that performed penetration testing for LabMD. CX0051 (Providyn Service Solutions Proposal for LabMD, executed by M. Daugherty). Mr. Davidson executed ProviDyn's Certification of Records of Regularly Conducted Activity. CX0470 (Providyn Certification of Records of Regularly Conducted Activity).

26. Allen Truett, former Chief Executive Officer of Automated PC Technologies, Inc.

Mr. Truett was the Chief Executive Officer of Automated PC Technologies, Inc., a business that provided services to LabMD starting in approximately 2001 or 2002. CX0731 (Truett Dep. Tr.) at 25. Mr. Truett's company provided services to LabMD until approximately March 2007. *Id.* at 49-50.

27. Peter Sandrev, Broadvox employee, Cypress Communications, LLC ("Cypress") designee

Cypress Communications provided technology services to LabMD starting in approximately 2004 through March or April 2012. CX0729 (Sandrev, Cypress Comm. Designee, Dep. Tr.) at 13, 19. Before 2009, Cypress provided LabMD with telephone services and broadband internet services. *Id.* at 26. LabMD switched to Voice Over IP Protocol (VOIP) telephony in 2009, *id.* at 13, while continuing its broadband internet service. *Id.* at 26. Cypress did not provide security or other services within LabMD's network. *Id.* at 51, 60-61.

Other Individuals and Entities

28. Robert Boback, Chief Executive Officer of Tiversa Holding Corporation ("Tiversa"), Tiversa designee

Mr. Boback is CEO of Tiversa. CX0703 (Boback, Tiversa Designee, Dep. Tr.) at 11. Tiversa provides information security services, such as breach detection and remediation. *Id.* at 10. Tiversa specializes in finding breaches on peer-to-peer networks. *Id.* at 10-11. In February 2008, Tiversa found and downloaded a file containing information from LabMD ("the 1718 file"). *Id.* at 24-25. In 2008, Tiversa reached out to LabMD regarding its discovery of the 1718 file. *Id.* at 77-78. Tiversa downloaded the 1718 file on three more occasions (*id.* at 57, 63), and it found the file "in multiple locations" as recently as November 2013. *Id.* at 9-10.

29. Erick Garcia

Mr. Garcia was arrested by the Sacramento police on October 5, 2012. CX0720 (Jestes Dep. Tr.) at 25. At that time, he was found to be in possession of LabMD documents. *Id.* at 23. He pled "no contest" to California state charges of identity theft. *Id.* at 44.

30. Christina Heide, Acting Deputy Director for Health Information Privacy, Office for Civil Rights, or other designee, U.S. Department of Health and Human Services ("HHS")

Ms. Heide, or another designee of HHS, may testify about the existence or non-existence of any evaluations by HHS of LabMD's compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the regulations promulgated under HIPAA and HITECH.

31. Karina Jestes, Detective, Sacramento, CA Police Department

Detective Jestes is a detective with the Sacramento Police Department who specializes in property crimes, which includes identity theft. CX0720 (Jestes Dep. Tr.) at 6, 12. On October 5, 2012, Detective Jestes conducted a search of 5661 Wilkinson Street in Sacramento. *Id.* at 17-18. The search of that property turned up checks made out to LabMD as well as LabMD "Day Sheets" containing names and Social Security numbers of consumers whose Personal Information was maintained by LabMD. *Id.* at 23, 33-35.

32. M. Eric Johnson, Dean of Owen Graduate School of Management, Vanderbilt University

Dean Johnson is the Dean of the Business School at Vanderbilt University. CX0721 (Johnson Dep. Tr.) at 9. Prior to assuming his position at Vanderbilt in July 2013, he was a Professor at the Tuck School of Business at Dartmouth College and Director of the Center for Digital Studies. *Id.* at 6. In 2009, Dean Johnson published an article titled *Data Hemorrhages in the Health-Care Sector*. *Id.* at 14-15. The article includes information about finding a 1,718 page LabMD document containing patient SSNs, insurance information and treatment codes for thousands of patients on a peer-to-peer network. *Id.* at 103-104.

33. David Lapides, Detective, Sandy Springs, GA Police Department

Detective Detective Lapides is a Detective with the Sandy Springs Police Department. CX0723 (Lapides Dep. Tr.) at 10. LabMD filed a report with the Sandy Springs Police Department on March 27, 2013. *Id.* at 14. Detective Lapides was assigned to follow-up on the report. *Id.* at 16. On April 2, 2013, Detective Lapides spoke to LabMD's counsel, Mr. Fusco, who stated that he believed a former LabMD employee, [redacted] had stolen LabMD documents that were found in Sacramento. *Id*. at 21-23. Detective Lapides conducted an investigation and found no evidence that [redacted] stole the documents found in Sacramento. *Id.* at 31.

34. Jonn Perez, Trend Micro Inc. employee

Mr. Perez is an employee of Trend Micro, Inc. Mr. Perez signed Certifications of Records of Regularly Conducted Activity produced by Trend Micro. CX0341 (Trend Micro Certifications of Records of Regularly Conducted Activity); CX 0352 (Trend Micro Certifications of Records of Regularly Conducted Activity).

35. Matt Wells, Trend Micro Inc. employee

Mr. Wells is an employee of Trend Micro., Inc. Mr. Wells signed Trend Micro, Inc.'s Certification of Records of Regularly Conducted Activity. CX0341 (Trend Micro Certifications of Records of Regularly Conducted Activity) at 3.

36. Euly Ramirez, Supervisor, Sacramento, CA Police Department

Ms. Ramirez is the Supervisor of the Records Division of the Sacramento Police Department. Ms. Ramirez signed the Sacramento Police Department's Certifications of Regularly Conducted Activity. CX0086 (Sacramento Police Department ("SPD") Certification of Records of Regularly Conducted Activity (2nd Production)); CX0089 (SPD Certification of Records of Regularly Conducted Activity (1st Production)); CX0588 (SPD Certification of Records of Regularly Conducted Activity (Forensic Disc)).

37. Kevin Wilmer, Investigator, Federal Trade Commission, Bureau of Consumer Protection, Division of Privacy and Identity Protection

Mr. Wilmer is an investigator at the Federal Trade Commission. CX0732 (Wilmer Dep. Tr.) at 143. Mr. Wilmer analyzed the Social Security numbers appearing in the Sacramento documents to determine the Social Security numbers were being or had been used by people with different names. *Id.* at 146-151; CX0451.

Expert Witnesses

38. Raquel Hill, PhD

Professor Hill is an Associate Professor at Indiana University, School of Informatics and Computing, and a Visiting Scholar at Harvard University's School of Engineering and Applied Science, Center for Research on Computation and Society.

CX0740 (Hill) ¶¶ 9-10. Her research focuses on trust and security for distributed computing environments and privacy of medical related data. *Id.* at ¶¶ 8, 10.

Professor Hill will testify, from her perspective as an expert in computer security, data privacy, and networking systems, regarding whether LabMD: (1) failed to provide reasonable and appropriate security for consumers' personal information within its computer network and (2) could have corrected any such security failures at relatively low cost using readily available security measures. *Id.* ¶¶ 49-106.

39. Rick Kam, CIPP/US

Mr. Kam is a Certified Information Privacy Professional (CIPP/US), and is the President and Co-Founder of ID Experts, a company specializing in data breach response and identity theft victim restoration. CX0742 (Kam) at 3, 5. In this role, Mr. Kam has had the opportunity to work on data breach incidents as part of ID Experts' incident response team, which has managed hundreds of data breach incidents, protecting millions of affected individuals and restoring the identities of thousands of identity theft victims. *Id.* at 3.

Mr. Kam will testify, from his perspective as an expert in identifying and remediating the consequences of identity theft and medical identity theft, about the risk of harm, particularly from medical identity theft, to consumers whose sensitive personal information LabMD disclosed without authorization; and about consequences of the risk of unauthorized disclosure caused by LabMD's failure to provide reasonable and appropriate security for consumers' personal information. *Id.* at 8, 19-23.

40. Clay Shields, PhD

Professor Shields is a Professor in the Computer Science Department at Georgetown University. CX0738 (Shields Rebuttal Expert Report) at 4. He has

expertise in networking and network protocols, computer security, digital forensics, responding to network and computer system events, and peer-to-peer networks. *Id.* at 4, 6-7. He received his bachelor's degree in Electrical Engineering from the University of Virginia. *Id.* at 5. He earned both his Master's degree and Ph.D at UC Santa Cruz. *Id.* at 5.

Professor Shields will testify from his perspective as an expert in networking and network protocols, computer security, digital forensics, responding to network and computer system events, and peer-to-peer networks, regarding whether: (1) the disclosure of LabMD files on the Gnutella peer-to-peer network; (2) the manner in which LabMD files could be located on the Gnutella network using the LimeWire program; and (3) the expertise and resources required to locate the files. *Id.* at 4-5, 14-34.

41. James Van Dyke

Mr. Van Dyke is the Founder and President of Javelin Strategy & Research ("Javelin"). CX0741 (Van Dyke) at 1. Among other services, Javelin produces an annual study of identity theft in the United States. *Id.* . Under Mr. Van Dyke's leadership, Javelin's study provides a comprehensive analysis of identity fraud in the United States. *Id.*

Mr. Van Dyke will testify, from his perspective as an expert in identity theft, regarding the risk of injury to consumers whose personally identifiable information has been disclosed by LabMD without authorization and to consumers whose personally identifiable information was not adequately protected from unauthorized disclosure. *Id.* at 2-3, 6-14.

Exhibit 3

LabMD IT Employees