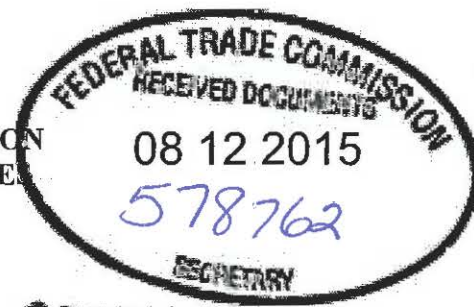


UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION  
OFFICE OF ADMINISTRATIVE LAW JUDGE



\_\_\_\_\_)  
In the Matter of )  
 )  
LabMD, Inc., )  
a corporation, )  
Respondent. )  
\_\_\_\_\_)

PUBLIC

Docket No. 9357

ORIGINAL

**COMPLAINT COUNSEL'S CORRECTED\* POST-TRIAL BRIEF**

Alain Sheer  
Laura Riposo VanDruff  
Jarad Brown  
Ryan Mehm  
Megan Cox

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

Complaint Counsel

\* Complaint Counsel inadvertently omitted an attachment from its Post-Trial Brief filed August 10, 2015: a revised proposed Notice Order referenced on page 76, note 11 of both Complaint Counsel's August 10, 2015 Post-Trial Brief and this Brief. This document, Complaint Counsel's Corrected Post-Trial Brief, includes the proposed Notice Order as Attachment 1, and is otherwise identical.

## TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
TABLE OF AUTHORITIES .....	v
EXECUTIVE SUMMARY .....	1
1. RESPONDENT.....	5
1.1 Company Basics.....	5
1.1.1 LabMD’s Collection and Maintenance of Consumers’ Personal Information.....	6
1.1.1.1 LabMD’s Collection and Maintenance of Consumers’ Personal Information from Physician-Clients .....	7
1.1.1.2 LabMD’s Collection and Maintenance of Consumers’ Personal Information Directly from Consumers.....	8
1.2 LabMD’s Computer Network.....	10
1.2.1 Servers and Other Equipment on LabMD’s Computer Network.....	10
1.2.2 Employee Computers on LabMD’s Computer Network.....	11
1.2.3 LabMD’s Network from January 2014 to Present.....	12
1.2.4 Computer Equipment Provided by LabMD to Physician- Clients Connected to LabMD’s Network .....	12
2. LABMD’S MEASURES TO PROTECT PERSONAL INFORMATION ON ITS NETWORK WERE NOT REASONABLE.....	13
2.1 LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Networks .....	13
2.2 LabMD Did Not Have a Comprehensive Information Security Program.....	15
2.2.1 A Written Comprehensive Written Information Security Program is a Roadmap for Achieving Reasonable Security .....	15
2.2.2 LabMD’s Did Not Have a Comprehensive Written Security Program.....	17
2.2.3 When LabMD Finally Prepared Written Information Security Policies in 2010, They Were Incomplete.....	18
2.2.3.1 The Written Policies Prepared by LabMD in 2010 Failed to Address Key Security Policies.....	18
2.2.3.2 LabMD Did Not Enforce Policies In The Manuals .....	19
2.2.4 LabMD Could Have Developed, Implemented, and Maintained a Comprehensive Information Security Program At Relatively Low Cost.....	21
2.3 LabMD Did Not Use Reasonable, Readily Available Measures to Identify Commonly Known or Reasonably Foreseeable Security Risks and Vulnerabilities .....	22
2.3.1 Risk Assessment Is a Critical Component of a Comprehensive Information Security Program .....	22

2.3.1.1	Warnings And Comprehensive Information About Known Or Reasonably Foreseeable Vulnerabilities Were Readily Available To LabMD From Government And Private Sources.....	23
2.3.1.2	Many Tools Are Available to Assess and Remediate Risks.....	24
2.3.2	LabMD Did Not Implement Automated Scanning Tools.....	25
2.3.3	LabMD Did Not Use Penetration Testing Before 2010.....	26
2.3.3.1	Penetration Tests Revealed That LabMD’s Servers Were Vulnerable to Attack .....	27
2.3.3.1.1	LabMD’s Mapper Server Had Multiple Vulnerabilities Related to the Transfer of Sensitive Information from Physician Clients.....	28
2.3.3.1.2	LabMD’s Mapper Server Had Vulnerabilities In The Database Application LabMD Used to Maintain and Retrieve Sensitive Information .....	30
2.3.4	LabMD Could Not Effectively Assess Risks Using Only Antivirus Applications, Firewalls, and Manual Inspections.....	31
2.3.4.1	LabMD’s Use of Antivirus Software Could Not Reliably Detect Security Risks Because It Did Not Consistently Update Virus Definitions, Run Scans, or Review Scans.....	31
2.3.4.1.1	Antivirus on Servers .....	32
2.3.4.1.1.1	Inadequate Virus Definition Updating.....	32
2.3.4.1.1.2	Inadequate Scanning and Scan Reviews.....	33
2.3.4.1.2	Antivirus on computers used by employees and physician client offices.....	33
2.3.4.1.2.1	Inadequate Virus Definition Updating.....	33
2.3.4.1.2.2	Inadequate Scanning and Scan Reviews.....	35
2.3.4.2	LabMD’s Firewall Could Not Reliably Detect Security Risks.....	36
2.3.4.3	LabMD’s Manual Inspections Could Not Reliably Detect Security Risks.....	38
2.4	LabMD Did Not Use Adequate Measures to Prevent Employees From Accessing Personal Information Not Needed to Perform Their Jobs.....	40
2.4.1	Access Controls .....	40
2.4.2	Data Minimization .....	41
2.5	LabMD Did Not Adequately Train Employees to Safeguard Personal Information.....	42
2.5.1	LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information .....	42
2.5.2	LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information .....	43
2.6	LabMD Did Not Use Common Authentication-Related Security Measures .....	45
2.6.1	LabMD Did Not Establish or Implement Policies Prohibiting Employees From Using Weak Passwords .....	45
2.6.2	LabMD Did Not Implement Strong Password Policies for Its Servers.....	47

2.6.3	LabMD Allowed Weak Passwords to be Used on Computers Placed in Physician-Clients' Offices.....	48
2.6.4	LabMD Did Not Disable the Accounts of Former Users .....	48
2.6.5	LabMD Did Not Implement Two-Factor Authentication to Compensate for Weak Passwords.....	49
2.7	LabMD Did Not Maintain and Update Operating Systems and Other Devices.....	49
2.7.1	LabMD Did Not Update Devices and Programs .....	50
2.8	LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information.....	52
2.8.1	LabMD Employees Were Given Administrative Access to Workstation Computers .....	52
2.8.2	LabMD Stored Backups of Personal Information on an Employee Workstation.....	53
2.8.3	LabMD Did Not Reasonably Deploy Firewalls.....	55
2.8.3.1	LabMD Did Not Fully Deploy Network and Employee Workstation Firewalls.....	56
2.8.3.2	LabMD Did Not Properly Configure Its Firewalls to Block Unnecessary Ports.....	57
3.	PEER-TO-PEER FILE SHARING APPLICATIONS .....	57
3.1	Operation of Peer-to-Peer File Sharing Applications .....	58
3.2	Risk of Inadvertent Sharing Through Peer-to-Peer File Sharing Applications .....	60
4.	SECURITY INCIDENTS .....	61
4.1	LimeWire Installation and Sharing of 1718 File .....	61
4.2	Sacramento Incident.....	62
5.	LABMD'S DATA SECURITY PRACTICES CAUSED OR ARE LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS THAT IS NOT REASONABLY AVOIDABLE BY THE CONSUMERS THEMSELVES AND IS NOT OUTWEIGHED BY COUNTERVAILING BENEFITS TO CONSUMERS OR COMPETITION .....	63
5.1	LabMD's Unreasonable Security Practices Caused or Are Likely to Cause Substantial Injury to Consumers .....	63
5.1.1	LabMD's Security Failures Placed All Consumers Whose Personal Information is on Their Network at Risk of Substantial Harm.....	67
5.1.2	Substantial Consumer Injury from Unauthorized Disclosure of the 1718 File .....	68
5.1.2.1	Potential Identity Theft from Exposure of the 1718 File .....	69
5.1.2.2	Potential Medical Identity Theft From Exposure of the 1718 File	70
5.1.2.3	Reputational and Other Harms from Exposure of the 1718 File ...	71
5.1.3	Substantial Consumer Injury From Unauthorized Disclosure of the Sacramento Day Sheets and Copied Checks.....	71

5.2	The Harm Caused or Likely to Be Caused By LabMD’s Failures is Not Reasonably Avoidable by Consumers Themselves .....	72
5.3	The Harm Caused or Likely to be Caused by LabMD’s Failures is Not Outweighed by Countervailing Benefits to Consumers or Competition.....	73
6.	COMPLAINT COUNSEL’S PROPOSED ORDER IS APPROPRIATE AND SHOULD BE ENTERED .....	76
6.1	Fencing-In Relief is Appropriate .....	77
6.2	The Notice Order is Reasonably Related to LabMD’s Unlawful Practices and is Clear and Precise.....	82

## TABLE OF AUTHORITIES

**Statutes**

15 U.S.C. § 45..... 1

**Regulations**

Standards for Safeguarding Consumer Information, 16 C.F.R. § 314.4..... 83

Statement of Basis and Purpose, Debt Settlement Amendments to Telemarketing Sales Rule, 75 Fed. Reg. 48458 (Aug. 10, 2010)..... 63

**Cases**

*Chicago Bridge & Iron Co. N.V. v. FTC*, 534 F.3d 410 (5th Cir. 2008)..... 82

*Cont'l Wax Co. v. FTC*, 330 F.2d 475 (2d Cir. 1964)..... 82

*Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152 (9th Cir. 2012)..... 72

*FTC v. Accusearch, Inc.*, 2007 WL 4356786 (D. Wyo. Sept. 28, 2007)..... 73, 85

*FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009)..... 73, 76

*FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830 (Stip. Prelim. Injunct.) (D.D.C. Nov. 3, 2014)..... 86

*FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373 (D. Conn. 2009)..... 76

*FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048 (C.D. Cal. 2012)..... 76

*FTC v. Cornerstone & Co., LLC*, Case No. 1:14-CV-01479 (Stip. Prelim. Injunct.) (D.D.C. Sept. 10, 2014)..... 86

*FTC v. Direct Mktng. Concepts, Inc.*, 648 F. Supp. 2d 202 (D. Mass. 2009)..... 77, 80, 87

*FTC v. Kennedy*, 574 F. Supp. 2d 714 (S.D. Tex. 2008)..... 66

*FTC v. Nat'l Lead Co.*, 352 U.S. 419 (1957)..... 82

*FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104 (S.D. Cal. 2008)..... 66, 73, 74, 75

*FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010)..... 72

*FTC v. RCA Credit Services, LLC*, 727 F. Supp. 2d 1320 (M.D. Fla. 2010)..... 76, 87

*FTC v. Ruberoid Co.*, 343 U.S. 470 (1952)..... 77

*Jacob Siegel Co. v. FTC*, 327 U.S. 608 (1946)..... 77, 82, 85

*Kraft v. FTC*, 970 F.2d 311 (7th Cir. 1992)..... 77

<i>N. Tex. Specialty Physicians v. FTC</i> , 528 F.3d 346 (5th Cir. 2008).....	82
<i>Orkin Exterminating Co., Inc. v. FTC</i> , 849 F.2d 1354 (11th Cir. 1988) .....	73
<i>Porter &amp; Dietsch, Inc. v. FTC</i> , 605 F.2d 294 (7th Cir. 1979) .....	82
<i>Remijas v. Neiman Marcus Group, LLC</i> , No. 14-3122, 2015 U.S. App. LEXIS 12487 (7th Cir. July 20, 2015).....	63, 66
<i>Sears, Roebuck &amp; Co.</i> , 676 F.2d 385 (9th Cir. 1982).....	78, 81, 82
<i>Telebrands Corp. v. FTC.</i> , 457 F.3d 354 (4th Cir. 2006) .....	81
<i>Thompson Med. Co. v. FTC</i> , 791 F.2d 189, 192 (D.C. Cir. 1986) .....	82
<i>U.S. v. Bldg. Insp. of Am.</i> , 894 F. Supp. 507 (D. Mass. 1995).....	80
<i>U.S. v. Consumer Portfolio Services, Inc.</i> , Case No. 8:14-cv-00819-ABC-RNB (Stipulated Order for Perm. Injunct.) (C.D. Cal. June 11, 2014).....	83
<i>Warner-Lambert Co. v. FTC</i> , 562 F.2d 749 (D.C. Cir. 1977).....	86

#### **Administrative Materials**

<i>Alternative Cigarettes, Inc.</i> , No. C-3956, 2000 FTC LEXIS 59 (Apr. 27, 2000) (consent order)	87
<i>Apple, Inc.</i> , No. 122-3108, Statement of Comm’r Maureen K. Ohlhausen (Jan. 15, 2014).....	73
<i>Body Sys. Tech., Inc.</i> , 128 F.T.C. 299 (Sept. 7, 1999) (consent order).....	87
<i>Brake Guard Prods., Inc.</i> , 125 F.T.C 138 (1998).....	81, 87
<i>Canandaigua Wine Co.</i> , 114 F.T.C. 349 (June 26, 1991) (consent order) .....	87
Comm’n Order Denying Resp’t’s Mot. to Dismiss (Jan. 16, 2014) .....	63
<i>Consumer Direct, Inc.</i> , No. 9236, 1990 FTC LEXIS 260 (May 1, 1990) (consent order).....	87
<i>Cytodyne LLC</i> , 140 F.T.C. 191 (Aug. 23, 2005) (consent order).....	87
<i>Daniel Chapter One</i> , 2010 FTC LEXIS 11 (2010).....	83
<i>Indoor Tanning Ass’n.</i> , 149 F.T.C. 1406, 1439 (May 13, 2010) (consent order).....	87
<i>Int’l Harvester Co.</i> , Docket No. 9147, 104 FTC 949, 1984 WL 565290 (1984) .....	passim
<i>MaxCell BioScience, Inc.</i> , 132 F.T.C. 1 (July 30, 2001) (consent order).....	87
<i>Oreck Corp.</i> , 151 F.T.C. 289 (May 19, 2011) (consent order).....	86
<i>Phaseout of Am., Inc.</i> , 123 F.T.C. 395 (Feb. 12, 1997) (consent order).....	87
<i>Pom Wonderful LLC</i> , Docket No. 9344, Initial Decision (May 17, 2012).....	passim

*PPG Architectural Finishes, Inc.*, Docket No. C-4385, 2013 FTC LEXIS 22 (Mar. 5, 2013) (consent order) ..... 86

*Snore Formula, Inc.*, 136 F.T.C. 214 (July 24, 2003) (consent order) ..... 87

*Third Option Labs., Inc.*, 120 F.T.C. 973 (Nov. 29, 1995) (consent order) ..... 87

*Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6 (1984)77, 78, 79, 81

*Wasem's, Inc.*, Docket No. C-2524, 1974 FTC LEXIS 134 (July 23, 1974) (consent order) ..... 86

**Other Authorities**

Financial Institutions and Customer Information: Complying with the Safeguards Rule..... 84

FTC Bureau of Consumer Protection Business Center: Data Security..... 84

Protecting Personal Information: A Guide for Business..... 84



## EXECUTIVE SUMMARY

The evidence in this matter establishes conclusively that LabMD's unreasonable data security practices put at risk the medical, financial, and other sensitive Personal Information of hundreds of thousands of consumers. By not taking reasonable measures to protect consumers' most sensitive personal information, LabMD exposed that information – including Social Security numbers and medical testing information – to people who had no right to see it, both within and outside LabMD. LabMD's unreasonable data security practices, have caused and are likely to cause substantial consumer injury that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or competition, in violation of the FTC Act's prohibition of "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). Moreover, the company's inadequate security practices are likely to continue causing such injury to consumers unless this Court enters an order requiring the company to adopt reasonable data security practices. Accordingly, LabMD violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, and it is appropriate to enter an order requiring it to, among other things, adopt a comprehensive information security program, obtain biennial security assessments, and notify consumers it has placed in harm's way.

LabMD's business model depended on gathering the most sensitive types of Personal Information about hundreds of thousands of consumers, who often were not aware that LabMD was receiving and indefinitely storing their information. Not only did it obtain their Social Security numbers along with their names and addresses, as well as information about their health insurance, it also gathered and continues to maintain sensitive health information, such as health testing codes that can reveal the consumer was tested for sexually transmitted diseases. Because the exposure of such information can result in substantial and devastating consumer injury, a company that receives and stores such information has a duty to take reasonable steps to protect

this consumer data in a manner appropriate to its extreme sensitivity. LabMD, a multi-million dollar business holding the sensitive data of more than 750,000 consumers, failed in that duty.

Taken together, the comprehensive mountain of evidence introduced by Complaint Counsel in this case conclusively proves that LabMD acted unreasonably for a business holding a vast amount of sensitive data in failing to reasonably secure consumers' Personal Information.. LabMD's failures are multiple and systemic. And in the rare instances in which LabMD took some nominal action to attempt to address the security of consumers' sensitive Personal Information, its measures were woefully inadequate. Specifically, LabMD:

- failed to have a comprehensive written information security program;
- failed to use reasonable, readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities
- failed to use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- failed to adequately train employees to safeguard personal information;
- failed to require employees to use common authentication-related security measures;
- failed to maintain and update operating systems and other devices; and
- failed to employ readily available measures to prevent or detect unauthorized access to personal information.

LabMD failed to implement many key data security practices, and when it did act regarding data security, it used inadequate and sloppy measures. For example, rather than using automated tools that check every corner of an employee's computer, LabMD performed walk-around inspections of its employees' computers that were haphazard, disorganized, and reactive.

Unsurprisingly, LabMD's hit-or-miss visual inspections failed to discover that LimeWire, an unauthorized and unnecessary P2P file sharing application, was running on the computer used by LabMD's billing manager between 2005 and 2008, and that hundreds of LabMD files, the 1718 File, a file containing the most sensitive types of Personal Information of over 9,300 consumers, were available for sharing from that computer.

LabMD's conduct – both its failures to act and inadequate steps it did take – is particularly injurious to consumers given the vast amounts of highly sensitive information in its possession. LabMD's business is predicated on collecting and maintaining on its computer network and elsewhere the most sensitive of consumers' Personal Information: their names linked with (1) dates of birth, addresses, and Social Security numbers; (2) their medical diagnoses and health insurance information; and (3) their financial information, such as credit card numbers and expiration dates and bank account and routing numbers. When this highly sensitive and personal information is exploited, consumers are likely to suffer a wide range of harms, including identity theft, medical identity theft, and disclosure of sensitive private medical information.

The fact that LabMD holds the sensitive personal information of hundreds of thousands of consumers while maintaining unreasonable data security exposes those consumers to a likelihood of harm that they cannot reasonably avoid, and that is not outweighed by benefits to consumers or competition. Often, it is only a matter of time before those unreasonable security practices lead to security incidents. Unreasonable data security practices create opportunities for others to exploit computer system vulnerabilities, obtain consumers' sensitive information, and misuse that information. LabMD's overall unreasonable data security practices were likely to cause substantial injury to the hundreds of thousands of consumers whose sensitive information

LabMD maintains on its networks. Further, LabMD's practices led to at least one known security incident when, despite years of warnings and public attention about the risks of peer-to-peer file sharing, the 1718 File, a file containing extremely sensitive personal information of approximately 9,300 consumers, was made available on a peer-to-peer network and was downloaded from a LabMD computer using off-the-shelf, standard peer-to-peer software. A second security incident occurred when the Sacramento Police Department discovered identity thieves in possession of LabMD "Day Sheets" containing sensitive personal information, such as names, Social Security numbers, and in some cases, diagnosis codes, and copies of personal checks from consumers made payable to LabMD.

Rather than demonstrate the reasonableness of its data security practices, LabMD has attempted to make this litigation only about the exposure of the 1718 File, claiming that it was "stolen" when in fact, as LabMD's witness Mr. Wallace testified in response to LabMD's questioning, it was freely available from a LabMD computer to anyone, anywhere using LimeWire. No special skills or technologies were needed to view or download the 1718 File from LabMD's computer. LabMD has zeroed in on this exposure with an obsession rivaling Inspector Javert, spinning a web of conspiracy theories dripping with innuendo and unsupported allegations. In an attempt to shift the focus from its own extensive security failures, LabMD points a finger at everyone but itself. However, Mr. Wallace testified clearly, unambiguously, and with no contravention, that the 1718 File was freely available on a peer-to-peer network for anyone to download using off-the-shelf, standard peer-to-peer software. Far from advancing LabMD's case, Mr. Wallace's testimony completely undermined LabMD's finger-pointing and further reinforced what the evidence has shown all along: LabMD's unreasonable security practices resulted in the 1718 File – a clear-text document containing the most sensitive Personal

Information of 9300 consumers – being maintained in a file designated for sharing on a LabMD computer on which LimeWire had been installed. As a result, it was freely available from that computer along with other LabMD files to LimeWire users. This exposure, along with the exposure of nearly 10,000 consumers' Personal Information in the Sacramento Day Sheets and copied checks, are examples of the vulnerability of consumers' Personal Information maintained by LabMD as a result of LabMD's woefully inadequate security, and the likelihood that consumers would suffer harm as a result of LabMD's actions.

In short, LabMD's unreasonable security caused or is likely to cause substantial injury to the over 750,000 consumers whose Personal Information is maintained on LabMD's computer networks, including the nearly 10,000 consumers whose Personal Information was disclosed in the 1718 File and the Sacramento Day Sheets and copied checks. There is no way consumers could have learned about LabMD's security practices or avoided these potential injuries independently. LabMD's unreasonable data security practices did not benefit consumers or competition. Accordingly, LabMD violated Section 5 of the FTC Act. As described below, entry of the order accompanying the complaint is appropriate under these circumstances, and necessary to protect consumers whose information LabMD still holds.

## **1. RESPONDENT**

### **1.1 Company Basics**

LabMD is a privately held Georgia corporation. CCFF ¶¶ 54-55. Its business is conducting clinical laboratory tests on urological specimen samples from consumers and reporting test results to physicians. CCFF ¶ 50. Michael Daugherty is the Chief Executive Officer, President, and sole owner. CCFF ¶¶ 56, 305. LabMD provided services, through its physician-clients, to consumers throughout the United States. CCFF ¶¶ 51-52, 92, 94, 98-99. In the course of that business, LabMD collected and retains the Personal Information of over

750,000 consumers, including approximately 100,000 consumers for whom it never performed any testing. CCFE ¶¶ 71, 78-79. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately \$35 to \$40 million dollars, and before 2013 its annual profit margin was approximately 25%. CCFE ¶¶ 57, 60.

In approximately December 2013, LabMD stopped accepting specimen samples and conducting tests. CCFE ¶ 63. It has not and does not intend to dissolve as a Georgia corporation, and continues to provide past test results to healthcare providers and collect on monies owed to it. CCFE ¶¶ 63-64. LabMD has operated out of locations at 1117 Perimeter Center West Drive (prior to April 2009) and 2030 Powers Ferry Road (from April 2009 through approximately January 2014) in Atlanta, Georgia. CCFE ¶¶ 67-68. LabMD currently operates out of Mr. Daugherty's personal residence and a condominium owned by Mr. Daugherty, both in Atlanta, Georgia. CCFE ¶¶ 66.

#### **1.1.1 LabMD's Collection and Maintenance of Consumers' Personal Information**

LabMD collects consumers' Personal Information from its physician-clients and directly from consumers. CCFE ¶¶ 81-82, 89, 117, 120, 130-131, 134-135, 140-141. The Personal Information LabMD collected and maintains includes but is not limited to first and last name, Social Security number, date of birth, home address, telephone numbers, laboratory test results and diagnosis or medical test codes, health insurance company name and policy number, bank routing and account numbers, and credit and debit card account numbers. CCFE ¶ 12. LabMD does not delete or destroy consumers' Personal Information, but maintains it indefinitely. CCFE ¶ 72. In addition to electronic storage on servers and computer equipment, ¶¶ 254-255, hundreds of boxes of paper records and over fifty boxes of patient specimens, including slides and tissue

samples, that had been stored at LabMD's business premises are now stored at Mr. Daugherty's personal residence. CCFE ¶¶ 75-76.

**1.1.1.1 LabMD's Collection and Maintenance of Consumers' Personal Information from Physician-Clients**

LabMD collected most of the Personal Information it maintains from its physician-clients. CCFE ¶¶ 89, 120. Physician-clients typically transmitted Personal Information electronically to LabMD's computer network through a File Transfer Protocol, commonly called FTP. CCFE ¶ 90. LabMD's IT staff set up the data transfer. CCFE ¶ 84. In some instances, LabMD retrieved Personal Information of all the patients in a physician-clients' database, regardless of whether LabMD performed testing for those patients, both initially and on an ongoing basis. CCFE ¶¶ 85-87. In other cases, physician-clients' offices entered consumers' Personal Information one consumer at a time for transfer to LabMD. CCFE ¶ 88. In yet other cases, physician-clients provided LabMD with Personal Information in paper form, which LabMD would enter into its system for electronic storage. CCFE ¶ 117.

In many cases, LabMD supplied computer equipment to its physician-clients, including computers and monitors. CCFE ¶ 102. For example, LabMD supplied computers to its client Southeast Urology Network, PC (SUN). CCFE ¶ 109. On an hourly basis, the Personal Information of all consumers on the SUN doctor's office network was sent to LabMD's network through the LabMD-supplied computer. CCFE ¶ 110. Likewise, LabMD's client Midtown Urology used LabMD-supplied computer equipment to transfer consumers' Personal Information to LabMD for approximately 80 to 90% of its 50,000 patients. CCFE ¶¶ 113-115.

Once Personal information had been downloaded to LabMD's network, physician-clients could order tests using LabMD's online portal. CCFE ¶¶ 92, 94. Physician-clients could order a test by searching for a patient on LabMD's network by patient name, Social Security Number, or

date of birth. CCFE ¶ 93. After LabMD performed the tests, physician-clients accessed test results through LabMD's web portal by searching the system using a patient's Personal Information, such as name, date of birth, or Social Security number. CCFE ¶¶ 98, 100.

In addition to using data in connection with testing, LabMD collected Personal Information from its physician-clients in connection with filing insurance claims. CCFE ¶¶ 119-120. The Personal Information LabMD collected to file insurance claims included names; addresses; dates of birth; gender; telephone numbers; Social Security numbers; health care provider names, addresses, and telephone numbers; laboratory tests, test codes, and diagnoses; clinical histories; and health insurance company names and policy numbers. CCFE ¶ 120.

LabMD generated "insurance aging reports" that showed accounts receivable that had not been paid by insurance companies. CCFE ¶¶ 122-124. These insurance aging reports are spreadsheets generated from data in LabMD's Lytec billing system, and included Personal Information such as names; dates of birth; and SSNs; the American Medical Association current procedural terminology ("CPT") codes for the laboratory tests conducted; and health insurance company names, addresses, and policy numbers. CCFE ¶¶ 124-125. LabMD's billing staff used the reports in connection with collecting payments from insurance companies. CCFE ¶ 128. Some billing employees could save insurance aging reports as PDF files. CCFE ¶ 127. The billing manager saved insurance aging reports to her computer. CCFE ¶ 126. The 1718 File is a PDF of an insurance aging report. CCFE ¶¶ 1354-1357, 1363, 1366-1367.

**1.1.1.2 LabMD's Collection and Maintenance of Consumers' Personal Information Directly from Consumers**

LabMD also received Personal Information directly from consumers in connection with consumers' payments. CCFE ¶¶ 130, 134-135, 140-141. To collect patient payments, LabMD printed patient statements from its Lytec billing database, mailed them to consumers, and gave



consumers the option of paying by credit card or personal check. CCFF ¶¶ 131-132. To pay by credit card, patients wrote their account number on the bottom of the statement and mailed it back to LabMD. CCFF ¶¶ 134-135. The billing department ran the card number, and then filed the statements in an unlocked file cabinet in an unlocked room to which anyone entering the building could have gained access. CCFF ¶¶ 135-137. LabMD retained the paper statements for years. CCFF ¶ 138. When patients mailed personal checks – which contain an account number and routing number, a name, and often an address and phone number – to LabMD, LabMD photocopied the check before scanning and depositing it. CCFF ¶¶ 140-142. After being scanned and deposited, the checks were stored in an unlocked drawer in a supply room for six months. CCFF ¶ 142. LabMD stored the photocopies of the checks in an unlocked file cabinet at LabMD’s Perimeter Center West location, and then at the Powers Ferry Road location in boxes in an open room that was regularly left unlocked. CCFF ¶¶ 143-145. LabMD has never destroyed any of the photocopies it has made of consumers’ personal checks, and has copies of hundreds of checks going back to its inception. CCFF ¶¶ 146-147. LabMD scanned some of its copied checks in order to archive them electronically. CCFF ¶ 148.

In connection with consumer payments, LabMD created Day Sheet transaction reports (Day Sheets) from its Lytec billing system. CCFF ¶¶ 150-151. These are spreadsheets of payments received from consumers that may include Personal Information such as name, Social Security number, provider number and place of service, diagnosis code, and information on the payment. CCFF ¶¶ 152-153. Day Sheets could be saved electronically to a computer or printed by any of LabMD’s billing employees, who printed them almost daily. CCFF ¶¶ 155-156. Copies of checks were attached to the Day Sheets. CCFF ¶ 154. LabMD retains Day Sheets indefinitely, and has all the Day Sheets it has created since it has been in business. CCFF ¶¶

157-158, 160. LabMD stored printed Day sheets in boxes kept in storage rooms that were unlocked until approximately until 2012. CCFF ¶ 159. LabMD scanned and saved some of the Day Sheets to its network in order to archive them electronically. CCFF ¶ 161.

## **1.2 LabMD's Computer Network**

LabMD has and uses a computer network to collect and maintain consumers' Personal Information from its physician-clients, receive orders for tests from health care providers, report test results to health care providers, file insurance claims with health insurance companies, prepare bills and other correspondence to physician-clients' patients, prepare medical records, store test results and diagnoses, and to access documents related to processing claims and payments. CCFF ¶¶ 163-170.

LabMD's computer network consisted of servers, computers used by employees, the hardware needed to allow connections among them and to the Internet, and software of various types. CCFF ¶ 164. In addition, LabMD supplied computer equipment to its physician-clients that were connected to its system. CCFF ¶ 164. From at least 2006, LabMD managed its network using in-house IT employees and did not rely on outside service providers for its network security. CCFF ¶¶ 173, 175, 178, 182-183, 185-186, 188, 190. LabMD operated similar networks at its Perimeter Center West and Powers Ferry Road locations. CCFF ¶ 165.

### **1.2.1 Servers and Other Equipment on LabMD's Computer Network**

LabMD's servers host various applications, including billing, laboratory, and email applications; it used its servers and applications in connection with collecting and maintaining Personal Information . CCFF ¶¶ 212-213, 220-221, 225-226, 231-232, 235-238, 242-244. LabMD used the Windows operating system for its servers. CCFF ¶ 214. In October 2006, some LabMD servers were running Windows NT 4.0, an out-of-date, unsupported version of the operating system. CCFF ¶¶ 216, 1005-1008. From August 2009 through September 2011, most

servers ran Windows 2005 through Windows 2008 operating systems, but some were running older systems. CCFF ¶ 217.

LabMD's Mapper server processed personal information transferred from physician-clients' offices into data useable by the laboratory system so that it could be maintained on LabMD's network. CCFF ¶¶ 220-221. Its LabNet server runs LabMD's LabSoft laboratory software, used to record laboratory services ordered and performed, including test results. CCFF ¶¶ 225-226, 229-230. LabSoft stores consumers' Personal Information in a database on the LabNet server, and retrieves information from the database as needed. CCFF ¶¶ 231-232. LabMD's Lytec server runs the Lytec billing software. CCFF ¶¶ 235, 237. Once testing of a tissue sample is completed, the Lytec server and application import the data from the LabNet server. CCFF ¶ 236. LabMD stores Personal Information on the Lytec server, which is available to billing department and IT personnel. CCFF ¶¶ 238-239. LabMD's other servers included a mail server, a Demographics server, and an HL7 server used to store archive copies of laboratory data. CCFF ¶¶ 243-244.

LabMD's network also included switches and routers to connect its servers and computers together and to allow them to connect to the Internet and other outside resources. CCFF ¶ 246. Finally, LabMD's network had a ZyWall firewall from approximately May 2006 to 2010, when it was replaced by a Juniper firewall. CCFF ¶¶ 247-249.

### **1.2.2 Employee Computers on LabMD's Computer Network**

LabMD's employees used desktop computers that were connected to its internal network to access resources on the network, including applications that provided access to Personal Information maintained on the network. CCFF ¶ 194-195. In addition to storing Personal Information on the network servers as described *supra*, LabMD maintained files containing

highly sensitive Personal Information on employee desktop computers. CCFE ¶¶ 196, 1354-1358, 1361, 1363, 1366-1367.

LabMD supplied laptop computers to its sales representatives, which could be used to log in to LabMD's network to determine whether a physician-client's requested test was pending or completed. CCFE ¶¶ 201-202. In addition, some LabMD employees could remotely access their computers on LabMD's network, including Personal Information on the network, using their home computer and a service called LogMeIn. CCFE ¶¶ 204-206, 210. LabMD had no security requirements for the home computers used to access its network. CCFE ¶¶ 208.

### **1.2.3 LabMD's Network from January 2014 to Present**

LabMD moved its network from its Powers Ferry Road location in January 2014 to Mr. Daugherty's residence and a nearby condominium owned by Mr. Daugherty. CCFE ¶¶ 251-253. Located at Mr. Daugherty's residence and networked together are switches, routers, servers, a firewall, workstation computers, printers, a scanner and an Internet connection. CCFE ¶ 254. The servers, which include the LabNet and Lytec servers, are located in the basement. CCFE ¶ 255. The condominium houses a workstation that can remotely connect to the Lytec billing server at the residence. CCFE ¶ 256.

### **1.2.4 Computer Equipment Provided by LabMD to Physician-Clients Connected to LabMD's Network**

LabMD provided computer equipment to some of its physician-clients to communicate with LabMD's internal network through the Internet to transmit Personal Information, order tests, and retrieve test results. CCFE ¶¶ 90, 92, 94, 98-99, 263-265, 273. Until January 2014, when LabMD stopped accepting new samples for testing, LabMD collected Personal Information through the networked computers. CCFE ¶¶ 63, 265, 269. LabMD did not have control over

how the computers were used, and did not collect networked computers when its relationship with a doctor's office ended. CCFE ¶¶ 267, 276-277.

**2. LABMD'S MEASURES TO PROTECT PERSONAL INFORMATION ON ITS NETWORK WERE NOT REASONABLE**

Despite the fact that LabMD collected highly sensitive information of hundreds of thousands of consumers, it did not reasonably secure that information. LabMD's failure to maintain reasonable security constitutes an unfair practice under Section 5 of the FTC Act.

Under Section 5(n), an unfair practice is one that (1) causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves, (3) and not outweighed by countervailing benefits to consumers or to competition. This brief will first describe the practices that Complaint Counsel alleges are unfair. It will then discuss how these practices meet the three prongs of the unfairness test.

**2.1 LabMD Failed to Provide Reasonable Security for Personal Information on its Computer Networks**

As a company holding the sensitive Personal Information of hundreds of thousands of consumers, LabMD failed to provide reasonable security for Personal Information on its computer networks taking into account the nature and amount of data maintained within its network, such as by employing a layered data security strategy using measures readily available to it during the relevant time period. CCFE ¶¶ 382, 395. Information security is a dynamic arms race. CCFE ¶ 384. IT practitioners implement security measures to prevent intrusions, and would-be intruders look for ways to break or circumvent each new security measure. CCFE ¶¶ 384-385, 390. The cycle of implementation and circumvention must be ongoing because intruders frequently discover ways to evade existing security measures. CCFE ¶ 385. Security

practices that inadequately prevent or detect unauthorized access to sensitive information allow for intrusions.

Implementing reasonable security requires a layered strategy that involves: 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. CCFF ¶ 388.

If there is only one protection mechanism in place, malicious actors try to find ways to circumvent the single protection mechanism to gain unauthorized access to a system. CCFF ¶ 390. Reasonable security requires deploying different mechanisms in a layered manner to combat the risks. CCFF ¶ 390. A layered approach reduces the likelihood that an attack will succeed by forcing the attacker to penetrate multiple security measures deployed at different layers of network. CCFF ¶ 391.

Reasonable data practices must take into account not only the size and components of a company's network, but also the volume and sensitivity of the information maintained with the network: the greater the sensitivity and volume of the information, the greater the need for enhanced security measures to provide reasonable security. CCFF ¶ 392. For LabMD, the relevant considerations include the large amounts of highly sensitive Personal Information, including Social Security numbers, medical insurance information, and medical diagnosis codes maintained on its network. CCFF ¶ 393.

LabMD failed to implement reasonable security in that it (1) failed to develop, implement, or maintain a written security program; (2) did not use readily available measures to identify risks, including measures to detect and prevent unauthorized access to its networks; (3) did not prevent employees from accessing personal information not needed to perform their jobs;

(4) did not adequately train employees; (5) did not establish and implement password policies; (6) did not update operating systems; and (7) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks.

## **2.2 LabMD Did Not Have a Comprehensive Information Security Program**

LabMD did not have a written comprehensive information security program, and thus could not adequately protect the most sensitive information about hundreds of thousands of consumers it had on its computer network. CCFE ¶ 397-401. Without a written comprehensive information security program, LabMD could not adequately provide guidance to those implementing the plan and those receiving training under it, record its current security goals and practices, facilitate changes to those goals and practices as security threats evolved, and communicate its security goals and practices to future employees. CCFE ¶¶ 399-400. As a result, LabMD's security practices were reactive, incomplete, ad hoc, and ineffective, leaving patients' sensitive information unreasonably vulnerable. CCFE ¶ 401.

### **2.2.1 A Written Comprehensive Written Information Security Program is a Roadmap for Achieving Reasonable Security**

A comprehensive information security program is a roadmap to identify the risks a company faces and to choose security measures that are reasonable under its circumstances. CCFE ¶ 398. It sets out a company's security goals, policies that satisfy those goals, and security measures and practices that implement the policies. CCFE ¶ 404. Reasonable security balances the severity of a vulnerability or threat and the harm that will result if it is exploited against the cost of measure(s) that remediate the vulnerability or threat. CCFE ¶ 406. LabMD did not have a comprehensive information security program to follow to achieve reasonable security. CCFE ¶ 412.

The universally accepted network security goals are the confidentiality, integrity, and availability of information and resources on a network. CCFE ¶¶ 428, 503-504, 767, 803; *see also* CCFE ¶ 404. Generally, confidentiality is preventing unauthorized access to information; integrity is preventing unauthorized changes to information; and availability is ensuring access to information when it is needed. CCFE ¶¶ 407-409; 504-06. LabMD knew or should have known of its obligation to meet these goals. They are set out in various publicly available information technology guidelines and requirements prevailing at the time, such as NIST guidelines put forth in 2002 and the HIPAA Security Rule, which beginning in 2005 required companies such as LabMD to take reasonable measures to protect the confidentiality, integrity, and availability of sensitive medical information on its network. CCFE ¶ 489-491 (NIST); 428 (HIPAA).

Besides these security goals, a comprehensive information security program includes security policies and implementing practices to achieve the goals. CCFE ¶ 404. Among other things, these policies and implementing practices tell employees how to select appropriate security measures to address threats and vulnerabilities based on the severity of the harm that will result if it is exploited against the cost of measure(s) to remediate the threat or vulnerability, monitor security measures to ensure that they are working and effective, and change the measures to address new threats as they appear. CCFE ¶¶ 404-411.

A program that is not comprehensive unnecessarily leaves open security holes. Appropriate security policies, and their implementing practices, are tuned to the specifics of the network to which they apply, including its structure, components, and size, and the amount and sensitivity of information on it. CCFE ¶ 392; *see also* CCCL ¶¶ 14-16.

In addition to being comprehensive in scope, an information security program should be written, so that current IT employees and contractors and other employees know both what they



are supposed to do and what was previously done, to avoid making the same mistakes twice.

CCFF ¶ 411.

### **2.2.2 LabMD's Did Not Have a Comprehensive Written Security Program**

LabMD did not have any written security program in place prior to 2010, let alone a comprehensive one. CCFF ¶¶ 415-417. And once it reduced its purported security policies to writing, they were not comprehensive, nor did they provide for reasonable security. CCFF ¶¶ 452-455. LabMD has claimed that its Employee Handbook, Compliance Program, and employee training set out reasonable written security policies. CCFF ¶ 420. However, these materials say almost nothing about security, and do not effectively serve any of the purposes of a comprehensive information security program. CCFF ¶¶ 422-443.

For example, the Employee Handbook lacked specific policies and practices to protect sensitive information from unauthorized access. CCFF ¶ 423. It did not include a policy requiring employees to encrypt sensitive information in emails, nor did it require employees to use unique, hard-to-guess passwords. CCFF ¶¶ 425-426, 919-923. And although the handbook refers to “specific measures” LabMD claims it took to comply with HIPAA’s privacy provisions, the handbook does not identify any security measures or specific policies related to them. CCFF ¶¶ 427-429. Nor could LabMD’s IT employees or owner and CEO identify any of the measures to which the handbook referred. CCFF ¶¶ 430-431. In sum, LabMD’s Employee Handbook failed to include relevant and key security policies.

LabMD’s Compliance Program was even less informative on security policies than the handbook. The contractor who prepared the compliance program explained that the program was not designed to include and, in fact, did not include any security policies at all. CCFF ¶¶ 437-48. Indeed, the program explicitly anticipates that LabMD would elsewhere develop and

implement security policies to keep sensitive consumer information secure and private. CCF ¶ 436.

Finally, despite LabMD's claims to the contrary, the evidence establishes that the company's employee training did not provide meaningful security training to anyone, as explained further below. *See* Sections 3.5 (LabMD Did Not Adequately Train Employees to Safeguard Personal Information), 3.5.1 (LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information), and 3.5.2 (LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information), below.

### **2.2.3 When LabMD Finally Prepared Written Information Security Policies in 2010, They Were Incomplete**

Although LabMD prepared two policy manuals in 2010, neither of these manuals comprises a comprehensive information security program, both because they failed to include important security policies and because LabMD did not enforce the policies in them. CCF ¶¶ 452-455, 458-480.

#### **2.2.3.1 The Written Policies Prepared by LabMD in 2010 Failed to Address Key Security Policies**

The essence of LabMD's business model was that making systematic, bulk downloads of sensitive consumer information to LabMD's network, including through LabMD-supplied computers, would make it easy for physicians to order tests. CCF ¶¶ 84-90, 102-105. LabMD set up and controlled this bulk transfer of information over the internet, using a FTP program its IT employees set up in its physician-clients' offices. CCF ¶ 90. Nonetheless, neither of LabMD's manuals included policies setting out how its employees were to prevent unauthorized access to vast amounts of sensitive consumer information while it was in transit from physician clients to LabMD. CCF ¶ 453.

Similarly, neither manual included policies addressing whether sensitive information received and generated by LabMD should be stored in an encrypted format and, if so, how to do so. CCF § 454. This lack is particularly acute when coupled with policies directing a manager to perform daily back-ups of sensitive billing information about thousands of consumers onto a workstation computer with unfettered internet access and other employees to store business documents on their computers. CCF §§ 460-462, 1071-1072.

Finally, although both manuals included policies referring to passwords, neither required employees to use hard-to-guess passwords or even explained how to create one, and neither prohibited reusing the same password. CCF §§ 919-923A consequence of these failures is that many employees with access to very sensitive consumer information used the same easy-to-guess passwords for years; for example, one employee used the password “labmd” from 2006 to 2013. CCF § 957. LabMD’s policies also did not address passwords for logging into the FTP program LabMD used to transfer sensitive consumer information from physician client offices to its network, with the result that passwords used by physician-clients’ offices often included the users’ initials, the username and password could be the same, and many users shared passwords. CCF §§ 974-983. Furthermore, LabMD’s employees set the FTP program up so that anyone could log in anonymously, that is, without using any password at all. CCF §§ 781-788.

### **2.2.3.2 LabMD Did Not Enforce Policies In The Manuals**

In addition, LabMD did not enforce or effectively enforce some security policies whose importance it recognized by including them in the manuals. CCF §§ 458-480. LabMD did not, for example, enforce policies to control downloading and installing programs from the internet by limiting the administrative rights employees had over their computers. CCF §§ 458-462. Under these policies, most employees were not to receive administrative rights to their computers. CCF § 458. In practice, however, these policies to limit user rights were all but

meaningless, as many, LabMD employees could install any programs they wanted on their computers because they were given full administrative rights to the computers. CCFE ¶¶ 1056-1057.

Similarly, LabMD did not effectively enforce a “Software Monitoring Policy” to detect and remove unauthorized programs that it claims to have implemented in 2002 and included in the 2010 LabMD Policy Manual (purportedly covering security practices in effect in 2007 and 2008). CCFE ¶¶ 465-467. As described more fully in the section below setting out LabMD’s inadequate risk assessment practices, the policy was enforced, if at all, through haphazardly conducted manual inspections of the Windows “add/remove” file on employee computers. CCFE ¶¶ 468, 677; *see also* Section 3.3.4.3 (LabMD’s Manual Inspections Could Not Reliably Detect Security Risks). LabMD’s failure to detect that LimeWire, an unauthorized file sharing application, had been installed and was used on the computer used by LabMD’s billing manager demonstrates the ineffectiveness of these inspections, and lead, along with other multiple systemic failings, to the 1718 File being available for sharing to users on the P2P network as late as 2008. CCFE ¶¶ 691-696.

Finally, both policy manuals include a recommendation, purportedly first made in 2004, that employees encrypt sensitive information included in emails. CCFE ¶¶ 474-476. LabMD’s IT employees have testified that LabMD had no email encryption policy between 2004 and August 2009. CCFE ¶ 477. And even if it had such a policy, it would not have mattered because LabMD did not provide its employees with tools or training to encrypt sensitive information in emails. CCFE ¶¶ 478-479. As a result, between 2004 and at least October 2006, an IT employee transmitted sensitive consumer information from LabMD’s network to the private AOL email account of LabMD’s owner and CEO without encrypting the information. CCFE ¶ 480.

In sum, by failing to have a written comprehensive security program, LabMD jeopardized: the confidentiality of sensitive information about hundreds of thousands of consumers; the integrity and accuracy of that information, opening the door to medical errors made in reliance thereon; and the availability of the information to physicians to use to treat consumers. *See* CCFE ¶ 404. Not surprisingly, because it did not have a security roadmap, the limited security measures LabMD implemented were *ad hoc* and were not layered to achieve reasonable security. *See* CCFE ¶ 410.

#### **2.2.4 LabMD Could Have Developed, Implemented, and Maintained a Comprehensive Information Security Program At Relatively Low Cost**

LabMD could have developed, implemented, and maintained a comprehensive information security program to protect consumers' Personal Information at relatively low cost. CCFE ¶¶ 1121-1124.

National experts have developed best practices for securing data, including electronic health data in particular, and have made their work available at no cost online from as early as 1997. CCFE ¶ 1122. Organizations that have provided this information include the National Research Council (NRC) and the National Institute of Standards and Technology (NIST). CCFE ¶ 1122.. These materials are comprehensive: they address many common security topics, including, but not limited to, authenticating users, restricting user access to information based on need, limiting user ability to install software, assessing risk, encrypting information while stored and in transit, logging access to information and system components, ensuring system and information integrity, protecting network gateways, and maintaining up-to-date software. CCFE ¶ 1123. Some even provide cross-references to specific laws, such as HIPAA, making it easy for a company to identify policies, procedures, frameworks, and tools to use to comply with a particular law. *See* ¶ 493. Using these materials, LabMD could have prepared a written and

comprehensive security roadmap at relatively low cost, by selecting and freely copying policies, procedures, frameworks, and best practices appropriate to its circumstances instead of starting from scratch. *See* CCFE ¶ 1124. It could have used the same materials to periodically update the program as vulnerabilities, technologies, and its network changed. *See* CCFE ¶ 1124.

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

#### **2.3.1 Risk Assessment Is a Critical Component of a Comprehensive Information Security Program**

In the IT field, companies identify threats and vulnerabilities on their networks, and weigh the risks they present to the confidentiality, integrity, and availability of information on the network through a process of risk assessment. CCFE ¶ 484. The sensitivity and amount of data a company maintains inform this process, CCFE ¶¶ 392, 406. Without adequate risk assessment, LabMD was blind to vulnerabilities intruders or insiders could exploit to obtain unauthorized access to sensitive information on its network, even for vulnerabilities it could have easily eliminated. CCFE ¶ 486. Knowing a network's vulnerabilities and the prospect of harm they present is essential for deciding which security measures are reasonable for the network. CCFE ¶ 485. Risk assessment is therefore a foundation of a comprehensive information security program and a layered approach to data security. CCFE ¶ 483.

Frameworks to identify, assess, and mitigate risk have been available since at least 1997 at no charge from various sources, such as the National Institute of Science and Technology ("NIST") and the Centers for Medicare and Medicaid Services ("CMS"). CCFE ¶¶ 405, 489-493. Private entities, such as the System Administration, Networking, and Security Institute ("SANS"), also provide IT practitioners with risk assessment information and training. CCFE ¶ 494-496. These free frameworks set out concepts companies can adapt as needed to identify and

prioritize vulnerabilities taking account of their circumstances, such as their network structures and the types and amounts of harm that would result if there were a breach. CCFF ¶ 489-496.

For example, beginning in 2002, NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) explained a nine step process, beginning with cataloging network resources (including hardware, software, information, and connections) to define the scope of risk assessment, moving through vulnerability identification and cost-benefit analyses of measures that could mitigate the risk of a vulnerability, and ending with security measure recommendations and a written record of the process. CCFF ¶ 491. These primary steps included methods and tools that could be used to perform them. CCFF ¶ 492 For example, “Step 3: Vulnerability Identification” defined the term vulnerability and recommended gathering information about known vulnerabilities in programs running on a network, such as from prior risk assessments, vulnerability databases, and warnings from program vendors, and testing for the presence of the vulnerabilities, such as by penetration testing or otherwise. CCFF ¶ 492. CMS used the NIST concepts to provide a similar framework for analyzing and managing vulnerabilities for entities subject to HIPAA and the Security Rule. CCFF ¶ 493.

#### **2.3.1.1 Warnings And Comprehensive Information About Known Or Reasonably Foreseeable Vulnerabilities Were Readily Available To LabMD From Government And Private Sources**

A wealth of information identifying commonly known or reasonably foreseeable vulnerabilities has been available for years. CCFF ¶¶ 499-511. Sources include alerts from software vendors and security companies, and software vulnerability databases compiled by private and government entities. CCFF ¶ 499-511 (vulnerability databases available from government and private sources); *see also* CCFF ¶¶ 1020, 1172 (alerts provides by vendors). These databases include the Common Vulnerabilities and Exposures (“CVE”), the Common

Vulnerability Scoring System (CVSS”), the US Computer Emergency Response Team (“US Cert”), and NIST’s National Vulnerability Database (“NVD”). CCF § 501-511. The CVE assigns to each known vulnerability a unique numerical identifier that is used to catalog and retrieve information about the vulnerability, including remediation measures in many instances. CCF § 502. The CVSS facilitates prioritizing vulnerabilities by calculating a numerical impact severity score between 0 and 10 for each vulnerability, taking into account factors such as how easy or hard it is to exploit the vulnerability and the resulting impact on confidentiality, integrity, and availability. CCF §§ 503-508. US CERT provides free technical assistance to networks and notifications of current and potential security threats. CCF § 510. The NVD is the U.S. government’s free one-stop-shopping software vulnerability management database, and includes the CVE dictionary, CVSS severity ratings, and additional analysis and information about known vulnerabilities. CCF § 509. For years, LabMD did not consult such sources to learn about vulnerabilities to look for on its network. CCF §§ 512, 521, 722.

### **2.3.1.2 Many Tools Are Available to Assess and Remediate Risks**

Many software tools – both free and paid – and hardware devices are available for detecting vulnerabilities on a network. CCF § Many Tools Are Available to Assess and Remediate Risks. These include antivirus programs, firewalls, vulnerability scanning tools, intrusion detection systems, penetration testing programs, and file integrity monitoring products. CCF §§ 514-518. These tools are routinely updated, using public and proprietary information, so that they can identify newly discovered vulnerabilities. CCF § 500-503, 529

However, no single device or tool can identify all the different types of vulnerabilities that may be present on a network. CCF § 514. An antivirus program, for example, can identify viruses on a network but not whether unauthorized programs are running on the network. CCF § 515. Similarly, file integrity monitoring products can identify changes in files that may



indicate that malware is on the network, but cannot identify or remove the malware. CCF § 516. External vulnerability scans and penetration tests can identify outdated software, security patches that have not been applied, administrative accounts that are using default passwords, and open ports, but not viruses that are present on the network. CCF § 515.

Generally, for each type of tool there are options based on price and functionality. CCF § 517. There are, for example, a number of branded antivirus programs, with each vendor offering versions that differ in price and functionality. CCF § 517. As a result, a network administrator can tailor risk assessment tools to appropriately balance cost and effectiveness, taking into account the amount and sensitivity of the information on his or her network. CCF § 518.

### **2.3.2 LabMD Did Not Implement Automated Scanning Tools**

LabMD did not use two of these tools – an intrusion detection system (“IDS”) and file integrity monitoring (“FIM”) – at all. CCF § 702, 710. An IDS analyzes large amounts of network traffic and issues alerts and warnings about threats and suspicious activity found in the traffic. CCF § 700-701. File integrity monitoring products identify changes in critical files that may indicate that malware is present on a network. CCF § 706. IT practitioners employed these mechanisms during the relevant time period, and use these alerts, warnings, and changes to assess whether there are risks on the network. CCF § 707, 1134.

Without automated tools, such as an IDS and file integrity monitoring products, LabMD could not adequately assess whether vulnerabilities these tools could identify were present on its network. CCF §§ 701, 708. An IDS could have examined the large volume of sensitive personal information that LabMD received from its computers in the offices of physician clients to determine whether the information also carried security risks. CCF § 700-701. Similarly, a file integrity monitoring product could have provided a warning that an unauthorized program,

such as LimeWire, was running on a computer on network. CCFE ¶ 709. LabMD could have implemented SNORT, a well-respected and widely used IDS, which has been available at no cost since 1998. CCFE ¶ 1134. Free file integrity monitoring products, such as Stealth and OSSEC, were available to LabMD during the Relevant Period. CCFE ¶ 1136.

### **2.3.3 LabMD Did Not Use Penetration Testing Before 2010**

Penetration tests, a type of automated scanning tool that analyzes a network's strengths and weaknesses, provide a "hacker's eye view" of the network by spotting certain types of vulnerabilities that hackers could exploit to obtain unauthorized access to sensitive information on the network. CCFE ¶ 715. Practitioners use penetration testing products to identify and analyze -- from outside a network -- vulnerabilities that may be present on the network. CCFE ¶ 719. For example, penetration tests of all the IP addresses on a network can identify programs and operating systems that have not been updated to correct or patch known vulnerabilities, programs still using vendor-supplied default passwords long after they should have been changed to secure passwords, open ports an intruder could use to enter or leave the network, and the computers on the network that will accept connection requests from computers outside the network. CCFE ¶ 718.

LabMD did not use penetration testing to analyze its network's strengths and weaknesses until 2010, even though penetration testing tools had been available to IT practitioners since at least 1997. CCFE ¶¶ 721, 1140. Examples of penetration testing tools include include Wireshark (released in 1998 under a different name), Nessus (free until 2008), and nmap (released 1997). CCFE ¶ 1140. Those products could have helped the company to identify vulnerabilities and correct significant risks. CCFE ¶ 1140. For instance, a penetration test of all IP addresses on the network would have identified vulnerabilities such as outdated software, security patches that had not been applied, and administrative accounts with default settings.

CCFF ¶ 1141. When LabMD did finally use penetration tests, its servers were found to be dangerously insecure. CCFF ¶¶ 743, 746-748. By failing to have penetration tests until 2010, the company blinded itself to whether vulnerabilities penetration tests could have identified were present on its network. CCFF ¶ 718. And when LabMD hired an outside IT service provider, ProviDyn, to conduct nine penetration tests in May 2010, the cost was a mere \$450. CCFF ¶ 1145.

### **2.3.3.1 Penetration Tests Revealed That LabMD's Servers Were Vulnerable to Attack**

ProviDyn, an independent security firm, conducted the 2010 tests using Nessus and other programs. CCFF ¶¶ 763, 784. ProviDyn's reports catalogued the known vulnerabilities that it found and used a standard industry classification system to rate the impact of exploiting each vulnerability on the confidentiality, integrity, and availability of information on LabMD's network. CCFF ¶¶ 736-742. The vulnerability classification system had five categories: Urgent Risk, Critical Risk, High Risk, Medium Risk, and Low Risk. CCFF ¶¶ 737-742. An urgent risk vulnerability on a server, for example, will allow a hacker to act as a network administrator and remotely control or compromise the entire server. CCFF ¶ 738. The 2010 penetration tests were limited to just the servers on LabMD's network; LabMD still does not know what vulnerabilities might have been found on employee computers. CCFF ¶ 726.

LabMD controlled the security practices used on seven of the tested servers. CCFF ¶ 733. ProviDyn found so many urgent, critical, and other vulnerabilities on four of these servers that it rated as "poor" the overall security of each server. CCFF ¶ 747. Among those compromised was the Mapper server that LabMD used to receive sensitive information about hundreds of thousands of consumers from physician clients. CCFF ¶¶ 746-747, 752-756.

The number of vulnerabilities found by the Mapper penetration tests, the server's poor overall security rating, the programs on the server that were at risk, and the consequences of exploiting the vulnerabilities all illustrate the inadequacy of LabMD's risk assessment practices. The May 2010 penetration test identified 32 vulnerabilities on Mapper, including one Urgent, one Critical, two High, and three Medium Risk vulnerabilities. CCFE ¶ 754. A second test in July 2010 detected 30 vulnerabilities on Mapper, including many of the May 2010 test vulnerabilities and a new Critical Risk vulnerability. CCFE ¶ 774. Both tests rated Mapper's security posture as "poor." CCFE ¶¶ 753-755. A third penetration test in September 2010 rated as Mapper's security posture as only "average." CCFE ¶ 756.

#### **2.3.3.1.1 LabMD's Mapper Server Had Multiple Vulnerabilities Related to the Transfer of Sensitive Information from Physician Clients**

Four of the Mapper vulnerabilities were in the FTP program that LabMD used to transfer sensitive information about hundreds of thousands of consumers from physician client offices to its network, and other vulnerabilities were in the database program that LabMD used to store, organize, and retrieve the information. *See* CCFE ¶¶ 759-797. Hackers can exploit these vulnerabilities to view and take data transferred by FTP – which in LabMD's case was sensitive Personal Information. *See* CCFE ¶¶ 762, 782. Some of these vulnerabilities were widely known years before being found by penetration tests of Mapper. *See* CCFE ¶¶ 786, 806-808.

The first FTP vulnerability is "Anonymous FTP Writeable root Directory," which is the Urgent Risk FTP vulnerability that ProviDyn detected during the May and July 2010 Mapper penetration tests. CCFE ¶¶ 759, 764. This vulnerability enabled an intruder outside the network to completely control the server and obtain consumer information from it. CCFE ¶¶ 762, 767. This vulnerability was first reported in 1993, and was included in the publicly available CVE database in 1999. CCFE ¶ 768. According to the CVSS, the vulnerability is easy to exploit, and

doing so will completely compromise the confidentiality, integrity, and availability of the server. CCFF ¶ 767. Corrective action is simple: restrict “write” access to the server’s root directory to only authorized users who have been authenticated by their unique credentials. CCFF ¶ 770.

The second FTP vulnerability is “FTP Writeable Directories,” which is the new Critical Risk vulnerability ProviDyn found in LabMD’s FTP program in the July 2010 penetration test. CCFF ¶ 774. It was not present during the first scan ProviDyn conducted in May 2010, thereby highlighting the benefit of regular, ongoing risk assessment to identify new vulnerabilities or old vulnerabilities that are new to a network. *See* CCFF ¶ 774. An intruder could exploit this flaw to host unauthorized information on Mapper, such as possibly illegal content. CCFF ¶ 775. According to the CVSS, the vulnerability is easy to exploit, and doing so will partially compromise the confidentiality and availability of the server. CCFF ¶ 776. This vulnerability was first identified in 1999. Harms from this vulnerability can be easily prevented by setting up the directories so that they are not world-writeable from outside LabMD’s network. CCFF ¶ 778.

The third FTP vulnerability, “Anonymous FTP Enabled,” is a Medium Risk vulnerability that ProviDyn detected during the May and July 2010 Mapper penetration tests. CCFF ¶¶ 781, 783. The tests found that the FTP program on Mapper was set up to allow anyone, including intruders, to log in to the program without having to enter a password or unique credentials. CCFF ¶ 782. Once logged in, an intruder could have opened any files that were available on Mapper, including files that contained sensitive consumer information. CCFF ¶ 782. The vulnerability was included in the publicly available CVE database in 1999. CCFF ¶ 786. The CVSS classified the vulnerability as easy to exploit, leading to partial compromise of the confidentiality of information on the server. CCFF ¶ 787. Appropriate corrective action has

been well-known for years: disable anonymous log ins, and periodically review files for sensitive information and restrict access to them. CCFF ¶ 788.

The last of the FTP vulnerabilities was “FTP Supports Clear Text Authentication.” CCFF ¶ 792. It is a Medium Risk vulnerability that ProviDyn detected during the May, July, and September 2010 Mapper penetration tests. CCFF ¶¶ 792, 795. The tests found that the FTP program was set up so that user credentials and data were transmitted in clear text rather than being encrypted. CCFF ¶ 793. User credentials were vulnerable to being intercepted using a traffic capture tool or a man-in-the-middle attack. CCFF ¶ 793. According to the CVSS, an intruder could use intercepted credentials to log in to the FTP program without authorization, partially compromising the confidentiality of information on the server. CCFF ¶ 796. A solution was to use a secure type of FTP program. CCFF ¶ 797.

#### **2.3.3.1.2 LabMD’s Mapper Server Had Vulnerabilities In The Database Application LabMD Used to Maintain and Retrieve Sensitive Information**

LabMD used a MySQL database program on the Mapper server to store, organize, and retrieve sensitive consumer information it received from its physician clients. CCFF ¶ 800. The May 2010 test detected several High Risk vulnerabilities in the MySQL program, including vulnerabilities from 2007 that could partially compromise the confidentiality, integrity, and availability of the program and its information. CCFF ¶¶ 802-803. The July 2010 test found a different High Risk vulnerability in the program, made public in 2009, again highlighting the benefit of regular, ongoing risk assessment. CCFF ¶¶ 804-805. These vulnerabilities all could have been corrected by installing an updated version of the MySQL program on Mapper. CCFF ¶¶ 806-808. LabMD did not do so.

### **2.3.4 LabMD Could Not Effectively Assess Risks Using Only Antivirus Applications, Firewalls, and Manual Inspections**

LabMD used only antivirus programs, firewall logs, and manual computer inspections to assess risk on its network. CCFE ¶ 524. These measures were inadequate to address risks for two reasons. First, as explained above, by relying exclusively on these three tools, LabMD limited the scope of its risk assessment to the types of vulnerabilities these tools were capable of identifying. CCFE ¶ 524. Second, LabMD implemented these tools inadequately. CCFE ¶¶ 527-696.

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

Antivirus software detects the presence of malicious software. CCFE ¶ 527, 532. While LabMD nominally installed antivirus software on its network, its use of the programs was ineffective to protect its network and the Personal Information it maintains for two primary reasons. CCFE ¶¶ 524, 527-536. First, it failed to update the software. CCFE ¶¶ 531, 539-550, 566-578, 612-618. The prevailing practice during this time period was to use up-to-date, current antivirus software. CCFE ¶ 530. Antivirus programs identify viruses using their individual fingerprints, which IT practitioners call signatures or definitions. CCFE ¶ 529. Since new viruses are discovered almost daily, their definitions must be added to antivirus programs before the programs can identify whether the new viruses are present on a server or computer. CCFE ¶ 529. LabMD did not consistently update virus definitions on its antivirus programs or verify that the definitions had been installed, with the result that the programs were at times incapable of determining whether new viruses had infected the servers and computers. CCFE ¶¶ 531, 539-550, 566-578, 612-618.

Second, LabMD failed to regularly run and review antivirus scans. CCFE ¶¶ 534-535, 553-557, 561-563, 590-596, 604-609, 621-623, 627. Using an antivirus program effectively

requires running it regularly to scan computers for known viruses, and consistently reviewing the scans and warnings to identify and correct the viruses that have been found. CCFE ¶ 533.

LabMD did not consistently run and review antivirus scans on servers and computers. CCFE ¶¶ 534-535, 553-557, 561-563, 590-596, 604-609, 621-623, 627. As a result, it was unreasonably blind to even those older viruses its programs were capable of discovering.

From at least 2004, LabMD used a variety of antivirus programs on servers, employee computers, and computers it operated in physician client offices. CCFE ¶528. As described below, for each of these programs, LabMD did not update definitions or consistently run and review them.

#### **2.3.4.1.1 Antivirus on Servers**

On servers, LabMD used the Symantec/Norton antivirus program between 2004 and 2006. CCFE ¶ 539. As previously described, LabMD used these servers for a variety of purposes, including to receive sensitive information about hundreds of thousands of consumers from physician clients using computers LabMD operated in client offices. CCFE ¶¶ 212-244, 540.

##### **2.3.4.1.1.1 Inadequate Virus Definition Updating**

The Symantec/Norton program as operated by LabMD did not consistently update virus definitions. CCFE ¶¶ 541, 544-546. Many LabMD servers could not receive new virus definitions because they did not have internet connections. CCFE ¶ 542. Furthermore, LabMD continued to use the program after Symantec/Norton ended support and stopped providing new definitions. CCFE ¶¶ 547-550.

As a result of LabMD's failures, APT, an independent security firm providing limited IT services to LabMD, found that the Symantec/Norton virus definitions on a LabMD server had not been updated for almost a year, from July 2005 to May 2006; LabMD could not know



whether new viruses discovered during that period had infected the server. CCFE ¶ 544. APT recommended installing a new antivirus program on servers in June 2006, but LabMD did not follow through for five months, until November 2006. CCFE ¶¶ 549-550. During that five month period, LabMD could not consistently determine whether new virus risks were present on any of its servers because Symantec/Norton ended support and stopped providing new definitions. CCFE ¶¶ 547-550.

#### **2.3.4.1.1.2 Inadequate Scanning and Scan Reviews**

Even if LabMD had ensured that the Symantec/Norton antivirus program was updating properly, its failure to consistently run virus scans on servers or review scan reports was unreasonable. CCFE ¶¶ 553-558, 561-563. The program did not automatically run regular scans, and at times, as APT observed in May 2006, it would not run a scan at all. CCFE ¶¶ 553-556. In addition, the Symantec/Norton program did not automatically report the results of scans to LabMD's IT employees. CCFE ¶ 561. Nor did the IT employees regularly run scans themselves and review them. CCFE ¶¶ 561-563. Instead, they ran reports, reviewed them, and then manually ran scans, *only* in response to server performance problems they observed or that an employee reported to them, such as trouble accessing a website. CCFE ¶ 563.

#### **2.3.4.1.1.2 Antivirus on computers used by employees and physician client offices**

LabMD continued these same poor practices with the free ClamWin and AVG antivirus programs it used on its employees computers and computers it operated in the offices of physician clients. CCFE ¶¶ 566-578, 581-587, 590-596, 599-601, 604-609, 612-618, 621-623, 626, 628-629.

#### **2.3.4.1.1.2.1 Inadequate Virus Definition Updating**

New virus definitions had to be installed manually on computers using the ClamWin program, one computer at a time, because the program did not support either automatic updating

or central management. CCFE ¶¶ 567-568. Central management allows IT employees to remotely update antivirus programs and virus definitions, run virus scans, review the scans, and take corrective actions. CCFE ¶ 569. LabMD relied on employees to visit the ClamWin website and download new virus definitions to their computers instead of having its IT employees update the definitions. CCFE ¶¶ 573-574. It did not train employees to update definitions, and, in any event, many could not have done so for want of an internet connection. CCFE ¶¶ 572, 575, 866-869, 872-876, 879-884, 887-891. The virus risk on these computers was nonetheless real, because LabMD permitted employees to use their own thumbdrives and CDs that could carry viruses to the computers. CCFE ¶ 576. Because it had no process requiring IT employees to regularly verify that employees had updated their virus definitions, ClamWin virus definition updating was unreliable and untimely, compromising risk assessment. CCFE ¶¶ 577-578. LabMD followed these same practices with the ClamWin programs on computers it operated in physician client offices, with the same poor results. CCFE ¶¶ 612-614.

LabMD's practices for updating virus definitions in the AVG program were only marginally better in that the program supported automatic updating. CCFE ¶¶ 581-587. The program did not, however, support central management, and LabMD did not require IT employees to regularly verify that virus definitions had been updated on the computers used by employees and in physician client offices that used AVG. CCFE ¶¶ 582-583, 615-616. Not surprisingly, the IT employee responsible between May 2010 and early 2014 for computers in physician client offices did not verify that the AVG program on those computers was updating virus definitions, even though vast amounts of sensitive consumer information was transmitted from those computers to LabMD's network. CCFE ¶¶ 104, 110, 112-115, 540, 616.

#### 2.3.4.1.2.2 Inadequate Scanning and Scan Reviews

Along with timely updating virus definitions, effectively using antivirus programs requires running virus scans to identify risks and then reviewing the scans to identify viruses that need to be corrected. CCFE ¶ 533. LabMD continued its practice of relying on each employee to manage the ClamWin antivirus program on his or her individual computer by expecting them to run ClamWin virus scans on the computers, even though it had no policy requiring them to do so or explaining how and when to run the scans. CCFE ¶¶ 572, 590-592, 866-869, 872-876, 879-884, 887-891.

Illustrative of LabMD's lack of policy, a former non-IT employee could not recall if there was even an antivirus program on her computer or how she used it, if at all. CCFE ¶ 594. In the same way that it lacked a process to verify that virus definitions had been updated, LabMD did not verify that employees ran ClamWin virus scans. CCFE ¶ 593. Because employees did not update definitions and run scans, the IT Department received PCs from LabMD employees that had viruses and malware on them. CCFE ¶ 596.

LabMD followed the same unreasonable scanning and verification practices for computers running the AVG antivirus program. The program allowed IT employees to schedule scans. CCFE ¶ 599. But, as with ClamWin, AVG did not support central management, and LabMD had no process to verify that the AVG antivirus program was operating properly and running scans. CCFE ¶¶ 583, 599-600. As a result, the IT employee responsible between May 2010 and early 2014 for computers in physician client offices did not verify that the AVG program was working correctly on those computers. CCFE ¶ 616. Instead, LabMD continued its unreasonable practice of waiting for employees or clients to complain about problems with their computers before checking to see if the antivirus program was working. CCFE ¶¶ 600-601.

LabMD's failure to ensure that the antivirus programs were working, that scans were run, and that employees timely forwarded scan results to its IT employees in a timely way put at risk computers used by employees and physician clients and the information on them. CCFE ¶ 524. Even when the programs were working and scanning for viruses, they did not automatically report infections to IT employees. CCFE ¶¶ 590, 599. IT employees inspected computers for infection only when employees or physician-clients complained about the performance of their computers. CCFE ¶ 605, 622. For example, after sales representatives received reports from physician clients that their computers were not working, LabMD's IT employees inspected the computers and found that they were infected with viruses and malware. CCFE ¶ 623. According to LabMD's IT employees, the ClamWin antivirus program was not an effective tool for removing infections, further compromising risk assessment. CCFE ¶ 595. Instead, the IT employees manually used other tools to disinfect the computers. CCFE ¶ 595.

#### **2.3.4.2 LabMD's Firewall Could Not Reliably Detect Security Risks**

Firewalls generally provide two primary security protections. First, traditional firewalls are designed to protect networks by blocking ports. CCFE ¶ 632. Since ports are associated with particular programs, blocking a port means that a program that uses that port cannot receive or send information. CCFE ¶ 631. LabMD's failures to adequately use firewalls to perform this function is discussed in section 3.8.3.2 (LabMD Did Not Properly Configure Its Firewalls to Block Ports), below.

Second, firewalls facilitate risk assessment by logging information about network traffic that IT practitioners review to assess risk. CCFE ¶ 642. Information in the logs can, for example, identify programs and computers on a network that are the targets for attempts at unauthorized access. CCFE ¶ 642. However, IT practitioners can learn little about risks from a firewall that can only log and store limited types and amounts of information. LabMD's

firewalls had only a limited capacity to contribute to risk assessment, and the company did not regularly use even that limited capacity to assess risks on its network. CCFE ¶¶ 643-648, 652-657.

Until the middle of 2010, LabMD used a simple ZyWall firewall to protect its network. CCFE ¶ 643. This firewall was inside the network. CCFE ¶¶ 164, 176, 638. LabMD connected to the Internet through a router, which was provided and managed by Cypress, LabMD's ISP. CCFE ¶¶ 164, 176. Cypress did not provide firewall or other security protections to LabMD's network, and the router was not configured to provide firewall protection. CCFE ¶ 178-180, 1086.

The types and amounts of network traffic information the ZyWall firewall could record and store was very limited. CCFE ¶¶ 643, 645. It could only record basic internet connectivity information, such as the IP address of a webpage an employee visited from a computer on LabMD's network. CCFE ¶ 645. Further, the firewall's memory was very small, so that it could only log such information about a few days' traffic. CCFE ¶ 643. It automatically overwrote, or erased, these logs every few days, when it ran out of memory. CCFE ¶ 644. As a result, unless LabMD systematically reviewed the logs every few days, the limited information in them would be lost forever and could not inform risk assessment.

Tellingly, no one reviewed LabMD's firewall logs on a regular basis between 2004 and mid-2009. CCFE ¶¶ 647-648. Instead, consistent with the company's reactive security posture, APT and LabMD's IT employees only reviewed the logs in response to complaints of problems, such as the internet being unavailable. CCFE ¶¶ 647-648. Because of the ZyWall firewall's limited logging capability and because LabMD did not regularly review the logs it had, the ZyWall firewall was not useful for risk assessment.

The software firewalls that were available through the Windows operating system that LabMD used on servers and computers could not compensate for the company's failure to review the ZyWall firewall logs to assess risk. As with the ZyWall hardware firewall logs, LabMD did not effectively use software firewalls for risk assessment. LabMD turned off software firewalls on its servers at times and did not enable software firewalls on employee computers. CCFF ¶¶ 1087 (servers), 1089-1091 (employee computers). Furthermore, LabMD had no regular practice to log or review activity on employee computers. CCFF ¶¶ 668-671, 675-676.

A number of free or low cost measures involving firewalls were available that would have allowed LabMD to identify commonly known or reasonably foreseeable security risks on its network. First, on August 25, 2004, Microsoft released Windows XP Service Pack 2, which included Windows Firewall, which LabMD could have deployed on employee workstations at just the cost of employee time. CCFF ¶ 1131. Second, LabMD could have used a free mechanism, Wireshark, to do packet level analysis to determine if Personal Information left the network without authorization, but did not do so. CCFF ¶ 1130. Finally, when LabMD finally implemented in 2010 a review of a monthly firewall log, that review only took a LabMD IT employee a maximum of ten minutes. CCFF ¶ 1129.

#### **2.3.4.3 LabMD's Manual Inspections Could Not Reliably Detect Security Risks**

Although LabMD asserts that it conducted manual inspections of computers to compensate for its lack of automated tools, any such assessments would be of limited value because they are conducted by people. CCFF ¶¶ 660-662 Furthermore, to the extent they happened at all, LabMD's manual inspections were haphazard and disorganized. CCFF ¶¶ 668-671, 675-677, 680-685. Even skilled IT practitioners cannot thoroughly identify vulnerabilities

on a computer by manually opening its files and programs and visually reviewing them for something out of the ordinary. CCFE ¶¶ 660-661. Computers are complex, with many places where vulnerabilities can hide without being visible to a human inspector. CCFE ¶¶ 660-661. Because of these inherent problems, security professionals recommend using automated risk assessment tools, such as an IDS, file integrity monitoring products, and penetration tests, for example, which can inspect computers during non-business hours or unobtrusively during use far more thoroughly than any human can. CCFE ¶ 662.

From at least March 2004 through at least when LabMD learned the 1718 File was available on a P2P network in May 2008,<sup>1</sup> LabMD did not inspect employee computers for vulnerabilities on a regular basis. CCFE ¶ 668. Instead, continuing LabMD's reactive approach to security, IT employees only manually inspected computers in response to employee complaints about computer performance. CCFE ¶¶ 668-671, 675-677. Given their haphazard deployment, LabMD's manual inspections never discovered that LimeWire, an unauthorized and unnecessary P2P file sharing application, was running on the computer used by LabMD's billing manager between 2005 and 2008, let alone that the 1718 File was available for sharing from that computer using the program. CCFE ¶¶ 691-695.

After learning about the sharing of the 1718 File in May 2008, LabMD confirmed that LimeWire was installed on the billing manager's computer, designated an employee as the IT Department desktop specialist and allegedly initiated new "Daily Walkaround" inspections. CCFE ¶ 680-681. To guide these inspections, LabMD claims to have prepared a checklist for IT employees to follow. CCFE ¶ 680-681. However, LabMD's IT employees, including its IT

---

<sup>1</sup> Ms. Simmons, who was employed at LabMD through August 2009 as an IT employee, CCFE ¶ 371-374, testified that she did not perform or see performed daily walkarounds. CCFE ¶ 668.

Department manager, did not follow any written checklist while walking around the office between early 2006 and September 2011. CCFE ¶¶ 682-684. Instead, they continued the ineffective practice of asking employees and clients if they were experiencing computer problems. CCFE ¶¶ 669-670, 675-676, 689. LabMD's "walkaround" inspections, like the prior inspections, would not necessarily have discovered whether LimeWire was installed on a LabMD computer. CCFE ¶ 696.

#### **2.4 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. CCFE ¶ 811. It also collected and maintained more information than it needed to conduct its business. CCFE ¶ 78-79, 832. Given the sensitivity and volume of the information it maintained, these practices needlessly increased the scope of potential harm resulting from a network compromise. CCFE ¶¶ 71, 78-79, 832, 835-841, 844-849.

##### **2.4.1 Access Controls**

As part of a reasonable data security strategy, companies that maintain sensitive information should restrict access to that data by defining roles for their employees and specifying the types of data that employees in those roles need. CCFE ¶ 812. 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. CCFE ¶ 813. Companies can use operating system functionalities and other applications to limit employees' access to information. CCFE ¶ 814. They can use Active Directory, for example, to automatically expire passwords, force employees to change them, and limit a user's access to programs or resources. CCFE ¶ 939. Because operating systems and



applications already have access controls embedded in them, rectifying this issue would have required only the time of trained IT staff and could have been done at relatively low cost. CCFE ¶ 1151.

LabMD did not control employees' access to sensitive information based on their job responsibilities. CCFE ¶¶ 817-821. In response to an interrogatory, LabMD was unable to specify the information to which any given employee had access, instead stating only that employees had "varying levels of access." CCFE ¶ 818. In fact, LabMD had taken no steps to prevent employees from accessing the sensitive information of consumers for which they had no business need. CCFE ¶¶ 819-821. For example, all billing personnel had full access to patient and lab databases, which allowed them to access all of a patient's Personal Information, including lab results. CCFE ¶ 820.

#### **2.4.2 Data Minimization**

In addition to allowing employees access to information that they did not need to perform their work, LabMD collected and maintained data which it did not need to conduct its business, even though IT practitioners during the relevant time period regularly purged unneeded data. CCFE ¶¶ 831-832. 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. CCFE ¶ 830.

LabMD had no policy for deleting data which it no longer needed and has not destroyed any patient information it has received from consumers since the company's inception. CCFE ¶¶ 835-841. In addition, LabMD collected and has maintained indefinitely Personal Information regarding approximately 100,000 consumers for whom it never performed testing and, therefore, whose information it had no business need to collect or maintain. CCFE ¶¶ 844-849.

## **2.5 LabMD Did Not Adequately Train Employees to Safeguard Personal Information**

Proper training is integral to a reasonable data security strategy because users are the weakest link in any information security program. CCFE ¶¶ 853-854. LabMD did not adequately train its employees to safeguard personal information, despite the types of Personal Information it held. CCFE ¶ 852.

### **2.5.1 LabMD Did Not Adequately Train IT Employees to Safeguard Personal Information**

Security training for IT employees is an essential part of reasonable security. Computer threats and vulnerabilities are always evolving, and IT practitioners must receive periodic training on the most recent advances in protecting against such threats. CCFE ¶ 857. Would-be intruders are constantly looking for new vulnerabilities to exploit in computers and programs to gain unauthorized access to consumers' Personal Information. CCFE ¶¶ 997-999. IT employees are the front line defense, and periodic training informs them about how to improve network security, including by identifying new vulnerabilities and attack methods and best practices to block them. CCFE ¶¶ 857-859.

LabMD did not provide its IT employees with information security training, formal or informal. CCFE ¶¶ 860-861. As a result, LabMD's security practices were reactive, incomplete, ad hoc, and ineffective. CCFE ¶ 863.

LabMD could have trained its IT employees to safeguard Personal Information at no or low cost. CCFE ¶ 1159. Several nationally recognized organizations provide free or low-cost IT security training courses. CCFE ¶ 1160. For example, the SysAdmin Audit Network Security Institute, founded in 1989, offers free security training webcasts. CCFE ¶ 1161. Additional free resources are available online. CCFE ¶ 1161. With these trainings, LabMD could have provided training to all staff on safeguarding Personal Information. CCFE ¶¶ 1159,

1162. Had LabMD availed itself of the numerous free resources available, providing employee training on safeguarding information would have required only the expenditure of time by LabMD staff. CCFE ¶ 1162.

### **2.5.2 LabMD Did Not Adequately Train Non-IT Employees to Safeguard Personal Information**

Non-IT employees are the weakest security link. CCFE ¶¶ 854, 1157. A company should provide its employees with training regarding any security mechanisms that require employee action—such as antivirus programs they must run themselves—or that employees are not technically prevented from reconfiguring. CCFE ¶ 867. Employees should also receive periodic training on acceptable use of computer equipment, current threats, and best practices. CCFE ¶ 868. Information security training is especially necessary where employees are given administrative access to equipment, because they can reconfigure the equipment in ways that could result in compromises such as downloading unauthorized software. CCFE ¶ 869.

As with its IT employees, LabMD failed to adequately train its non-IT employees to safeguard Personal Information. Non-IT employee training was especially important for LabMD because, for example, it expected non-IT employees to update virus definitions and run antivirus scans on their computers and gave some employees administrative rights to their computers, including the ability to change security settings. CCFE ¶¶ 568, 573-578, 583, 590-594, 604 (antivirus), 1056-1060 (administrative rights).

LabMD did not provide its non-IT employees, including sales representatives and billing employees, with any training regarding information security, security mechanisms, or the consequences of reconfiguring security settings in applications. CCFE ¶¶ 879-882. LabMD's IT employees did not provide such training either—the assistance they provided to colleagues was limited to, for example, how to use software and refill printers, or how to use IT to reduce the

employee's workload. CCFE ¶¶ 887-888, 890. Training for employees was critical, in part because many LabMD employees could change security settings on their computers using the administrative rights they were given. CCFE ¶ 880, 1056. Another example of the importance of training is that billing employees were able to access sensitive patient information, but were given no instructions about keeping that information private or on limiting their access to the information to that needed to perform their jobs. CCFE ¶ 882. The billing manager from 2005 through 2006 relied on training her employees received in their previous jobs, rather than providing training at LabMD. CCFE ¶ 883. The same billing manager supervised college students with no previous experience, and they were not provided training either—even though they had full access to the patient database. CCFE ¶ 884.

While LabMD provided its employees with “compliance training,” this training did not train LabMD employees about LabMD's information security practices, but merely stated that LabMD had obligations with regard to Personal Information and information security without providing employees any concrete guidance or instruction. CCFE ¶¶ 872-876. Likewise, LabMD's Employee Handbook and Compliance Program do not provide instructions on how to safeguard Personal Information, and do not contain specific policies about protecting data resources and infrastructure or explain what, if any, mechanisms LabMD implemented to achieve reasonable data security. CCFE ¶¶ 895-896. For example, although the Employee Handbook states that LabMD “has taken specific measures to ensure [its] compliance” with HIPAA, employees were not informed what these measures were and were given no specific instructions for complying with the law. CCFE ¶¶ 897-898. Furthermore, even assuming the 2010 Policy Manuals touch on data security to some minimal extent, employees did not receive any explanation or training on the Policy Manuals. CCFE ¶ 900.

## **2.6 LabMD Did Not Use Common Authentication-Related Security Measures**

As part of a reasonable data security strategy, companies should use strong authentication mechanisms to control access to employee workstations and other network resources. CCFF ¶ 903. With LabMD's network resources including the sensitive Personal Information of hundreds of thousands of consumers, protecting that information required reasonable authentication mechanisms. Without strong password policies, for example, an intruder may guess a weak password and use it to impersonate an employee and obtain unauthorized access to computers and information. CCFF ¶ 909. Authentication that a user is genuine and permitted access to a resource requires the user to provide information to the system that tells the system who they are and then proves that identity. CCFF ¶ 904.

Username and passwords are a common authentication mechanism. CCFF ¶ 905. Their effectiveness and security depends on two factors: the strength of the passwords, and how passwords are stored and managed. CCFF ¶ 906. Reasonable username and password authentication security can be achieved when policies and procedures are implemented to ensure that passwords are unique, strong, changed periodically, and stored securely. CCFF ¶¶ 906, 912, 914.

LabMD's authentication mechanisms were not reasonable for securing its network. CCFF ¶ 910. LabMD's IT employee Mr. Hyer acknowledged that when he joined the company in 2009 and applied his experience in data security practices at the time that LabMD's password policies were "less than adequate." CCFF ¶ 911.

### **2.6.1 LabMD Did Not Establish or Implement Policies Prohibiting Employees From Using Weak Passwords**

LabMD did not establish or implement password policies to ensure that strong passwords were being used to authenticate users and authorize them to access LabMD's network. CCFF

¶ 916. To promote the effectiveness of usernames and passwords, a company should have policies on the creation of strong passwords, such as imposing minimum length requirements for passwords, requiring special characters in passwords, dictating how long passwords can be used before they must be changed, and passwords to avoid. CCFF ¶ 914.

LabMD did not have written policies prohibiting using the username as the password, requiring password complexity, or prohibiting the use of dictionary words as passwords. CCFF ¶¶ 920-922. Before 2010, LabMD did not have a policy requiring a minimum password length for employees to access their workstation computers, and did not require users to include numbers or special characters in their passwords. CCFF ¶¶ 926-929. LabMD's own IT employee stated that when he joined in 2009, LabMD's passwords were "not as complex as they should have been," indicating that they did not meet the data security practices prevailing at the time. CCFF ¶ 913. And as of at least August 2009, LabMD did not enforce its purported policy requiring employees to change their password from the temporary default password assigned to them when they were first registered on the network. CCFF ¶ 930. LabMD also did not have a written policy prohibiting users from using the same username and password across applications. CCFF ¶ 923.

Furthermore, LabMD did not periodically review the strength of employee and client passwords and force password changes. CCFF ¶¶ 926-930, 955-957, 974-981. Until November 2010, LabMD did not use a computer process to require password strength and force password changes, despite the fact that a free centralized password management scheme, Active Directory, was built into the Windows operating system that LabMD had been using. CCFF ¶¶ 937-941. Prior to using centralized password management in November 2010, LabMD IT employees' only

means of ascertaining whether employees were using strong passwords was to verbally ask users for their passwords. CCFF ¶¶ 941-942.

As a result of LabMD's failure to adopt and adequately implement reasonable password policies, LabMD employees used weak passwords to access LabMD's network, both on site and remotely. LabMD employees used passwords that were not sufficiently complex, used only letters, were too short, and were easily guessed. CCFF ¶ 946-951. For example, LabMD Employee Sandra Brown used the username "sbrown" and the password "labmd" to access her LabMD computer when she worked on site at LabMD. CCFF ¶ 947. LabMD assigned her these credentials. CCFF ¶ 948. She later worked from home using her own computer and a service called Logmein.com to access LabMD's system, including patient databases, remotely—and used the same "sbrown" and "labmd" credentials. CCFF ¶¶ 949-950. Ms. Brown's weak credentials were not an anomaly—at least six employees used "LabMD" as a password. CCFF ¶¶ 951, 963.

Not only did LabMD employees use weak passwords, but they used them for years. CCFF ¶ 957. Before 2010, LabMD had no policy requiring the periodic changing of passwords. CCFF ¶ 955. Ms. Brown used her credentials "sbrown" and "labmd" unchanged from 2006 to 2013. CCFF ¶ 957. LabMD employees also shared authentication credentials, including passwords used to access Personal Information and logins to access computers on the LabMD network. CCFF ¶ 962. Sharing credentials was not an acceptable data security practice at the time, according to Mr. Hyer. CCFF ¶ 961.

### **2.6.2 LabMD Did Not Implement Strong Password Policies for Its Servers**

In addition to failing to implement and maintain reasonable password policies for employee access to workstation computers and other resources, LabMD did not implement and maintain reasonable policies for its network infrastructure, including servers. CCFF ¶¶ 968-971.

From October 2006 through April 2009, every server login username was “admin,” and every password was “LABMD.” CCFE ¶ 970. As of August 2009, LabMD’s LabNet server had a username of “admin” and the password was the dictionary word “bulldog.” CCFE ¶ 969. Dictionary words are inherently weak passwords. CCFE ¶ 915. Because LabMD had set up the system so that the server credentials were all linked to the same default administrator user profile, IT staff could not set up different user accounts with different credentials for each IT employee. CCFE ¶ 971.

### **2.6.3 LabMD Allowed Weak Passwords to be Used on Computers Placed in Physician-Clients’ Offices**

LabMD’s unreasonable password practices extended to the computers it provided to physician-clients for the transmission of Personal Information to LabMD. When computers were set up in physician-clients’ offices, the clients would submit the employees that needed access to the computers, and the credentials requested. CCFE ¶¶ 975-976. LabMD had no process to evaluate the complexity of the credentials, and would not reject any requested user credential no matter how simple or insecure. CCFE ¶¶ 976-977. For example, it was a common practice for nurses’ passwords to be their initials. CCFE ¶ 978. There was no prohibition on using the same credential as both the username and password or other combinations such as a username of a nurse’s initials and the password as the initials repeated twice. CCFE ¶¶ 980-981. In some instances, login credentials were shared among all employees in an office. CCFE ¶¶ 982-983. These practices placed the computers at risk of unauthorized access because the credentials were so easily guessed.

### **2.6.4 LabMD Did Not Disable the Accounts of Former Users**

In addition to failing to have or enforce policies regarding password complexity and expiration, LabMD did not disable the accounts of former users. Before August 2009, LabMD



failed to deactivate the login access of former physician-clients who no longer needed access to its network, and the former clients could still access the network. CCFE ¶ 986. In July 2010, an outside vendor conducted limited penetration tests of some of LabMD's servers. CCFE ¶ 987. The tests found several users whose passwords would never expire, including "Administrator," "Guest," and "asimmons." CCFE ¶ 987. Ms. Simmons, a LabMD IT employee, had left LabMD almost a year prior to the scan, in August 2009. CCFE ¶ 987. Accordingly, former employees like Ms. Simmons may have been able to access LabMD's network without authorization. CCFE ¶¶ 986-987.

#### **2.6.5 LabMD Did Not Implement Two-Factor Authentication to Compensate for Weak Passwords**

In addition to reasonable password practices, two-factor authentication is used as part of a layered data security strategy to reduce the risk of compromise. CCFE ¶ 991. It is often used in connection with remote login or access to highly sensitive data. CCFE ¶ 991. Two-factor authentication requires two forms of proof of a user's identity and authorization to access a resource, such as a password (something the user knows) and a biometric, such as a fingerprint or iris scan (something a user is), or a token (something the user possesses). CCFE ¶ 990. LabMD did not use two-factor authentication for remote users. CCFE ¶ 992. Two-factor authentication could have compensated for LabMD's failure to require the use of strong passwords for remote login. CCFE ¶ 993.

#### **2.7 LabMD Did Not Maintain and Update Operating Systems and Other Devices**

Maintaining and updating operating systems of computers and other devices to protect against known vulnerabilities is integral to a company's reasonable data security strategy. CCFE ¶ 997. Operating systems and programs are complex, and bugs, including security vulnerabilities, are inevitable. CCFE ¶ 998. Hackers exploit software bugs to gain unauthorized

access to computer resources and data such as that held by LabMD. CCFE ¶ 999. Given the value of the data LabMD holds, unauthorized access could have devastating consequences for consumers. CCFE ¶¶ 1642-1644, 1646-1650. To minimize the exploitation of bugs to gain unauthorized access, IT practitioners should connect to product notification systems and apply remediation processes and updates for vulnerabilities identified. CCFE ¶ 1171. These systems provide free notifications from vendors, as well as CERT, OSVDB, NIST, and others about newly discovered bugs and security vulnerabilities as well as patches and workarounds to resolve them. CCFE ¶¶ 1171-1172. Some vendors, such as Microsoft, issue updates and patches to fix software errors. CCFE ¶ 1173. In some instances, however, no patch is available because the vendor no longer supports the operating system or program. In these cases, resolving the vulnerability may require replacing the operating system or program with a newer version supported by the vendor.

### **2.7.1 LabMD Did Not Update Devices and Programs**

Through at least 2010, LabMD did not update its operating systems and other applications in a timely manner to address risks and vulnerabilities. CCFE ¶ 996. For example, some of LabMD's servers used the Windows NT 4.0 operating system for two years after Microsoft publicly warned users that it had stopped supporting it by issuing patches for vulnerabilities, acknowledged that it presented security risks, and recommended installing a newer operating system. CCFE ¶¶ 216, 1004-1007.

Another example is the Veritas backup application on LabMD's LabNet server, which stores and handles large amounts of consumers' sensitive Personal Information, including specific diagnoses and laboratory results. CCFE ¶¶ 1011-1012. When ProviDyn conducted a penetration test of the LabNet server in May 2010, it concluded that the overall security posture of the LabNet server was "Poor." CCFE ¶¶ 729, 746, 1014. In the May 2010 scan, ProviDyn

discovered two serious vulnerabilities in the Veritas application. First, the application was configured with the default administrative password—an issue that had been identified in a vendor advisory with a solution provided as early as August 15, 2005. CCFF ¶¶ 1017, 1019. ProviDyn identified the use of the default administrative password as a Level 5 Urgent Risk, which would allow an attacker to compromise the entire server running the Veritas application. CCFF ¶ 1018.

The second Veritas vulnerability was a “buffer overflow” vulnerability, a Level 4 Critical Risk that gave an attacker the ability to execute code remotely and take over partial control of the server. CCFF ¶¶ 1024-1026. By taking control of the server, a hacker could steal the Personal Information LabMD stored on it. CCFF ¶¶ 220-223, 225. A fix for this vulnerability had been made available as a free update in 2007 by the distributor of the software. CCFF ¶ 1028.

LabMD also failed to update its SSL 2.0, Secure Socket Layer protocol, for three years after Microsoft instructed users to remedy this vulnerability. CCFF ¶ 1031. SSL is the means by which data is encrypted during transmission over the Internet using HTTPS. CCFF ¶ 1032. The vulnerability provided hackers with access to information about the host server, including security settings. CCFF ¶ 1035. An attacker may be able to exploit the vulnerability to conduct man-in-the-middle attacks to intercept traffic or to decrypt communications to the affected servers, meaning a hacker could read the Personal Information physician-clients transmitted to LabMD. CCFF ¶ 90, 1037.

By the time ProviDyn found that LabMD’s LabNet and Mail servers were running this insecure version in May 2010 the program had been discontinued for several years. CCFF ¶¶ 1033-1034, 1036. Microsoft provided instructions on how to disable SSL 2.0 as early as April 23, 2007, and LabMD could have easily addressed this vulnerability by following instructions

provided by Microsoft. CCFE ¶¶ 1038, 1040. Microsoft also released Windows Server 2008 in February 2008 and recommended that users upgrade to this operating system to address the SSL 2.0 flaw. CCFE ¶ 1039.

## **2.8 LabMD Did Not Employ Readily Available Measures to Prevent or Detect Unauthorized Access to Personal Information**

LabMD failed to employ readily available measures to prevent or detect unauthorized access to Personal Information on its computer network. A reasonable data security strategy must include mechanisms that attempt to prevent the exploitation of vulnerabilities by an attacker, and to detect unauthorized access when an attack is successful; this process of detection enables an organization to identify holes in its security system and to patch them. CCFE ¶¶ 1045-1046. For a company like LabMD, which maintains the sensitive Personal Information of hundreds of thousands of consumers, reasonable security required that it employ methods and mechanisms to detect and prevent such access.

### **2.8.1 LabMD Employees Were Given Administrative Access to Workstation Computers**

Part of a reasonable data security strategy should include giving employees limited control over their computers by assigning them non-administrative access to their workstations, which prevents the downloading of software that could compromise both the workstation and their employers' entire network, including the Personal Information stored on it. CCFE ¶¶ 1050-1052. Administrative rights give employees full control over their computers. CCFE ¶¶ 1051, 1053, 1056-1057. With administrative rights employees can change security settings on their computers, such as turning off a software firewall, and installing unauthorized programs, such as LimeWire, that could compromise their computers as well as the network. CCFE ¶¶ 1056-1057, 1061.

Although the Windows operating system used by LabMD included functionality that would have allowed LabMD to assign its employees non-administrative rights, CCFE ¶¶ 1054, 1181, until at least November 2010, most LabMD employees had administrative rights on their workstation computers and could change their security settings. CCFE ¶ 1056. LabMD compounded this security risk by making it easy for employees to download and install unauthorized programs. CCFE ¶¶ 1057-1061. It allowed some employees unrestricted Internet access that they could use to visit any website and freely download files and programs to their computers. CCFE ¶¶ 1059-1060. Even employees without unrestricted Internet access could install programs and save files to their workstations from a USB memory stick or a disk. CCFE ¶ 1058. As a result of this failure to restrict employees' ability to install software, the file-sharing software LimeWire was installed on the billing manager's computer in or about 2005 and not discovered for years. CCFE ¶¶ 1061-1062. LabMD did not have any defined security measures that would have prevented sharing files from the billing manager's computer using LimeWire. CCFE ¶ 1063.

This is a problem LabMD could have easily solved. The Windows operating systems LabMD used included a program for assigning different levels of control to employees, including administrative rights and non-administrative rights. CCFE ¶¶ 1054, 1181.

### **2.8.2 LabMD Stored Backups of Personal Information on an Employee Workstation**

Backups should not be stored on employee workstations because an employee's workflow may inadvertently expose sensitive information to malicious software and unauthorized individuals. CCFE ¶¶ 1067-1068. Rather, to prevent unauthorized access to Personal Information as part of a reasonable data security strategy, backups containing Personal

Information should be stored on devices that are isolated from other employee activities. CCFE ¶ 1066..

However, LabMD actively stored backups containing Personal Information on employee workstations – its Policy Manuals, CX0006 and CX0007, both dictate that a daily backup of LabMD’s billing software should be stored to the Finance Manager’s desktop. CCFE ¶ 1070. The daily backup contained all of the patient, client, and billing information relating to LabMD’s work. CCFE ¶ 1071.

LabMD also stored copies of other files with highly sensitive Personal Information, including insurance aging files, on an employee’s workstation. CCFE ¶ 1072. As a result, this information was available to the Gnutella P2P network through the LimeWire file-sharing software installed on an employee computer that held these backups. CCFE ¶¶ 1363, 1367-1370, *see also* CCFE ¶ 1211, 1213.

Although no one can dispute the need to back up important information, LabMD’s back-up practices, on their own and especially in conjunction with its other security failures, unnecessarily increased the risk of unauthorized access instead of reducing it. For example, by failing to require employees to use hard-to-guess passwords, CCFE ¶¶ 920-923, 927-930, 945-951, 963, 955, 969-970, and giving managers administrative rights to their computers and unrestricted Internet access, CCFE ¶¶ 1056, 1058-1060, LabMD facilitated potential unauthorized access to computers where it stored back-ups of sensitive consumer information. CCFE ¶¶ 1069-1072. The back-ups, which included the most sensitive Personal Information, were not encrypted, as LabMD had no policy requiring encryption of anything. CCFE ¶¶ 73 (LabMD stored Personal Information on its network in unencrypted format); 454 (LabMD’s Policy Manuals did not describe whether sensitive information was to be stored in an encrypted

format); 474, 476-480 (LabMD did not provide tools for employees to encrypt emails containing sensitive information); 792-797 (FTP application on Mapper was not set up to encrypt its data and control connections, transmitting user name and password in clear text). Instead, it was LabMD's practice to store sensitive information unencrypted on its servers and employee computers. CCFE ¶ 73.

LabMD easily could have reduced the risk of unauthorized access to backed-up information by storing the information on a computer or device that was isolated from other computers and used for no purpose other than storing backed-up information. CCFE ¶ 1066. LabMD could have done so at low cost using a computer or device it already had. CCFE ¶ 1182.

### **2.8.3 LabMD Did Not Reasonably Deploy Firewalls**

As noted above, one function of a firewall is to protect a network or a computer by restricting traffic to and from the network or computer. CCFE ¶ 1075, 1080-1081. Information intended for a program running on a computer reaches that computer through the port that is used by that program. CCFE ¶ 1097. Specific ports are customarily assigned to and used by particular programs. CCFE ¶¶ 631, 635. Web servers and browsers, for example, customarily use ports 80 and 443 for world wide web traffic. CCFE ¶ 635. When a firewall is misconfigured so that ports for unnecessary programs are left open, the open ports provide avenues intruders can use to attack a network or computer. CCFE ¶ 633, 1097-1100.

Firewalls can be set up to block unwanted traffic to specific ports, and it is important to close all ports that do not need to be open for legitimate applications to prevent unauthorized access. CCFE ¶¶ 1098-1100. It is routine to configure firewalls to prevent unauthorized access by opening ports used by acceptable applications and closing ports used by unnecessary, unauthorized programs. CCFE ¶¶ 631-635, 1076. Additionally, IT practitioners have for years used penetration tests to identify firewall misconfigurations that leave open ports that should be

closed. CCFE ¶¶ 718-719, 1140, 1142. When a firewall is configured to block, or close, the port a program uses, the firewall discards any information that arrives for that port and the program that would use it. CCFE ¶ 1098. It follows that when ports for unnecessary programs are left open, the open ports can allow intruders to attack a network or computer. CCFE ¶ 633. Furthermore, a firewall that is not turned on provides no protection whatsoever for the network or computer it could protect.

It was common practice during (and after) the Relevant Period to protect a network and its servers and computers using hardware firewalls located at the network perimeter and software firewalls on individual devices. CCFE ¶¶ 1077-1079. Software firewalls can accommodate difficulties in implementing a perimeter, or gateway, firewall to block all unwanted traffic and then managing it by guarding against possible misconfigurations of the perimeter firewall and allowing more restrictive filtering on individual devices. CCFE ¶¶ 1080-1081.

#### **2.8.3.1 LabMD Did Not Fully Deploy Network and Employee Workstation Firewalls**

LabMD did not use firewalls to protect all equipment. For instance, the router that Cypress provided to LabMD to connect to the Internet had firewall capabilities that could have been used as a gateway firewall, but these capabilities were not enabled. CCFE ¶ 1086.

Even when LabMD had firewalls, they were disabled or not in use in some instances. For instance, LabMD disabled the software firewalls on some of its servers. CCFE ¶ 1087. On August 25, 2004, Microsoft released Windows XP Service Pack 2, an update to the operating system used on LabMD's computers from before 2005 through at least the beginning of 2010, which included a Windows Firewall for use on individual computers such as employee workstations. CCFE ¶¶ 1089-1090. From 2004 through March 2007, LabMD did not deploy or configure this included software firewall on its employee workstations. CCFE ¶ 1091. The



software firewalls were available for LabMD to use at no additional cost, requiring only proper configuration. CCFE ¶ 1183.

### **2.8.3.2 LabMD Did Not Properly Configure Its Firewalls to Block Unnecessary Ports**

For the firewalls that were active, LabMD did not configure them to block ports that it had no business need to keep open. For example, LabMD's Veritas backup software had a Level 5 vulnerability that could give an attacker administrative access to the software and the LabNet server running it, which would allow the attacker to control the server and its software and to retrieve files on the server. CCFE ¶ 233, 1102. In 2005, Symantec issued a warning recommending that Port 10,000 be closed until the Veritas backup application was updated to correct the security issue. CCFE ¶ 1103. In May 2010, five years after this warning, LabMD's Veritas backup software on its LabNet server had port 10,000 open. CCFE ¶ 1104. In fact, LabMD did not need *any* ports on the Veritas backup software to be open, because its backups were performed within its network and not across the Internet. CCFE ¶ 1105. LabMD could have addressed this vulnerability by closing the port, at the trivial cost of just employee time. CCFE ¶ 1183. Further, LabMD easily could have discovered the vulnerability and the open port years earlier by conducting routine penetration tests. CCFE ¶¶ 716, 718.

### **3. PEER-TO-PEER FILE SHARING APPLICATIONS**

The peer-to-peer (P2P) file-sharing software LimeWire was installed on the computer used by LabMD's billing manager. CCFE ¶ 1363. The software was used to participate in the Gnutella P2P network. CCFE ¶ 1363. As a result, LabMD placed the Personal Information of thousands of consumers at risk of exposure. CCFE ¶ 1367-1370. P2P file-sharing networks are networks of computers that allow users to search the computers of other users and download files from those computers. CCFE ¶ 1192, 1216-1217. P2P networks are often used to share music,

videos, pictures, and other materials. CCFE ¶ 1191. Files placed on a P2P network are made available for other users to freely come and take. CCFE ¶ 1193.

### **3.1 Operation of Peer-to-Peer File Sharing Applications**

The Gnutella P2P network consists of all the computers, commonly called peers, that are running a program to communicate with other peers over the internet using the Gnutella protocol, a language that specifies what messages can be sent between connected computers, the format of those messages, and the proper response to those messages. CCFE ¶¶ 1199-1200. A peer connects to the Gnutella network using software called a Gnutella client, which understands the Gnutella protocol and allows the peer to interact with other peers. CCFE ¶¶ 1192, 1199-1200. The Gnutella client involved in this case, LimeWire, is a popular client that was used by a wide variety of users to download and share files. CCFE ¶ 1207, 1363. Although it is common for peers to join and leave the network often, CCFE ¶ 1202, at any given time, the Gnutella network could have 2 to 5 million peers online. CCFE ¶¶ 1198.

A user shares files on the Gnutella network by designating a directory on his or her computer as a shared directory. CCFE ¶ 1211. The shared directory is typically designated when the client is installed and it is possible for a user to misconfigure a client by unintentionally selecting a directory to share that contains files that the user did not mean to share. CCFE ¶¶ 1211-1212. Once a directory has been selected to be shared, all files within that directory are made freely available for downloading by other users of the Gnutella network as long as the computer is on and connected to the Gnutella client. CCFE ¶ 1213-1214.

Users looking to download a file from the Gnutella network will typically search for files using search terms related to the file and will receive back a list of possible matches. CCFE ¶ 1216. The user chooses a file from the list and the file is then downloaded from other peers on the Gnutella network that possess the file. CCFE ¶ 1217. It is common for the folder that

receives downloaded files from the network to be the folder that is designated as the shared directory, so that downloaded files are immediately made available for further sharing. CCFF ¶ 1224-1225. Once the downloading peer has the file, the file can then be shared by that peer's computer without downloading it again. CCFF ¶ 1226. As a result, files downloaded from the network are often re-shared and begin to appear on other peers throughout the network. CCFF ¶ 1227. The Gnutella protocol has no mechanism to retrieve shared files or to prevent further sharing of shared files, so it is nearly impossible to remove a file from the network once it has been widely shared. CCFF ¶¶ 1229, 1231.

There are many ways that a malicious user who is looking for sensitive information on the Gnutella network can locate files that are likely to contain such information. CCFF ¶¶ 1273, 1276-1281. Users can search for a particular file using its file name, CCFF ¶ 1216, or its "hash" value,<sup>2</sup> CCFF ¶ 1220, 1269-1270. Malicious users can also search for files that are more likely to contain sensitive information by searching for a file extension of a file type that is often used to store sensitive information, such as ".pdf," and then sift through the results for files that look interesting. CCFF ¶ 1284-1288.

Malicious users can also locate peers that have been misconfigured to share more than the users intended, which are more likely to contain sensitive information. CCFF ¶ 1273-1281. They can do this by locating other sensitive files as discussed above or searching for files that are commonly kept in directories such as "My Documents" or C:\windows, which would indicate that a peer was sharing a large number of directories. CCFF ¶ 1279-1280. Once malicious users locate a file indicating that the peer was misconfigured, they can then use the browse host

---

<sup>2</sup> A hash is a long number computed based on all the data that makes up the file and is statistically unique to that file. CCFF ¶ 1220.

function, CCFE ¶ 1291-1296, to look through all the files that the peer is sharing and download any files that contain sensitive information. CCFE ¶ 1276.

In addition to the built-in features of Gnutella clients, it is relatively simple to create custom software that will perform searches using the Gnutella protocol. CCFE ¶¶ 1299-1300. It is not difficult to create custom software because most of the code required already exists. CCFE ¶ 1300. It would be relatively easy to create a piece of software that sought out Gnutella peers and used the browse host function to catalog the files available on the network. CCFE ¶ 1301. Such software is called crawler software and many programmers have produced crawler software with few resources. CCFE ¶ 1301-1304.

### **3.2 Risk of Inadvertent Sharing Through Peer-to-Peer File Sharing Applications**

Using P2P software creates a significant risk that files on a peer will be inadvertently shared with other users on the network. CCFE ¶ 1309-1311. The user may accidentally place files in the shared directory, or may inadvertently designate a folder containing sensitive information as the shared directory. CCFE ¶ 1310-1311. Research on inadvertent sharing through P2P networks was published in the early 2000s and the risks of P2P file sharing have been well known since at least 2006. CCFE ¶¶ 1316, 1321-1327, 1333-1335. By 2005, the US Computer Emergency Readiness team had published warnings about these risks, stating that “unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information.” CCFE ¶ 1333.

The Commission has published material aimed at educating both consumers and businesses about the risks of inadvertent sharing through the use of P2P software, as well as issuing a report and testifying before Congress to provide information on the subject. CCFE ¶¶ 1338, 1340-1342, 1345, 1347, 1349-1351. In 2003, the FTC released a publication called “File-Sharing: A Fair Share? Maybe Not,” which warned that consumers using P2P software

could “unknowingly allow others to copy private files you never intended to share.” CCFE ¶ 1340. In 2005, the Commission released a broader online security publication, “Stop. Think. Click,” which warned consumers that “you could open access not just to the files you intend to share, but to other information on your hard drive, like your tax returns, e-mail messages, medical records, photos, or other personal documents.” CCFE ¶ 1342.

In 2004, the Commission issued a joint business alert with the Council of Better Business Bureaus and the National Cyber Security Alliance, that included a warning that using P2P software could “lead to viruses, as well as a competitor’s ability to read the files on your computer.” CCFE ¶ 1345. The alert recommended “prohibiting your employees from installing file-sharing programs on their computers.” CCFE ¶ 1345.

In testifying before Congress in 2004, the Commission noted that P2P software presents a risk that sensitive personal files may be disclosed inadvertently. CCFE ¶¶ 1349-1350. In June 2005, Commission staff issued a report on P2P technology which included a section on the risks of P2P technology, including inadvertent sharing and the risk of downloading spyware and viruses. CCFE ¶ 1347. The Commission testified before Congress again in 2007 and addressed the risks created by P2P technology. CCFE ¶ 1351.

#### **4. SECURITY INCIDENTS**

##### **4.1 LimeWire Installation and Sharing of 1718 File<sup>3</sup>**

A copy of the Gnutella client LimeWire was installed on the work computer of LabMD’s billing manager, Rosalind Woodson, in or about 2005. CCFE ¶¶ 1363, 1366. The entirety of Woodson’s “My Documents” directory was shared by LimeWire and available for download by

---

<sup>3</sup> The assertions made on page 49 of Complaint Counsel’s pre-trial brief are not repeated here. Complaint Counsel’s post-trial brief and proposed findings of fact do not cite to Robert Boback’s testimony, CX0703, or to CX0019, nor do they cite to expert conclusions that were predicated on Mr. Boback’s testimony.

Gnutella users. CCFF ¶ 1368. This shared directory contained over 900 files, CCFF ¶ 1375, including LabMD's June 2007 Insurance Aging Report (the "1718 File"), a report that contains personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance policy numbers, and codes for laboratory tests conducted. CCFF ¶ 1361, 1367-1370. LabMD had no legitimate business need for LimeWire to be installed and had no security measures in place to detect or prevent P2P sharing from the billing manager's computer. CCFF ¶¶ 1371-1372. Despite the fact that it was well known within LabMD that Woodson had P2P software on her computer CCFF ¶¶ 1382-1390, the LimeWire client remained on the billing manager's computer until May 2008. CCFF ¶ 1364-1365, 1399-1400, 1404-1406.

Even then, it was not LabMD that discovered it was sharing patients' personal information on a P2P network, but a third party that found and downloaded the 1718 File on the Gnutella network in May 2008, along with other document. CCFF ¶¶ 1394-1395. The 1718 File was available for sharing by anyone using the Gnutella P2P network, and was found using off-the-shelf P2P software of the type available to any ordinary user. CCFF ¶¶ 1393-1394. After being notified of the 1718 File's availability on the P2P network, LabMD found the LimeWire client installed on the billing manager's computer and determined that it was sharing the 1718 File. CCFF ¶ 1399, 1402-1404. LabMD did not provide any notice to the patients' whose information was contained in the 1718 File. CCFF ¶ 1411.

#### **4.2 Sacramento Incident**

In October 2012, the Sacramento California Police Department found more than 35 LabMD "Day Sheets" and nine copied checks and one copied money order made payable to LabMD in the possession of individuals unrelated to LabMD's business who later pleaded no contest to state charges of identity theft. CCFF ¶¶ 1413-1414. Day Sheets are electronically-

generated reports relating to consumer payments from LabMD's billing application. CCFE ¶¶ 150-152. The Day Sheets contained the Personal Information of at least six hundred consumers, including names, Social Security numbers, and in some cases, diagnosis codes.

CCFE ¶¶ 1433-1434. Some of the Day Sheets post-date the 1718 File. CCFE ¶ 1354 (1718 File dated "6.05.07"), 1435 (some day sheets dated after June 5, 2007).

**5. LABMD'S DATA SECURITY PRACTICES CAUSED OR ARE LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS THAT IS NOT REASONABLY AVOIDABLE BY THE CONSUMERS THEMSELVES AND IS NOT OUTWEIGHED BY COUNTERVAILING BENEFITS TO CONSUMERS OR COMPETITION**

**5.1 LabMD's Unreasonable Security Practices Caused or Are Likely to Cause Substantial Injury to Consumers**

LabMD's failure to employ reasonable measures to protect consumers' extremely sensitive Personal Information caused or is likely to cause substantial injury to consumers. Section 5 recognizes that Complaint Counsel does not need to wait for harm to manifest before challenging conduct that is likely to cause consumer injury. Comm'n Order Denying Resp't's Mot. to Dismiss at 18-19 (Jan. 16, 2014) (requiring assessment of whether a company's "data security procedures were 'unreasonable' in light of the circumstances"); *see also, e.g.*, Statement of Basis and Purpose, Debt Settlement Amendments to Telemarketing Sales Rule, 75 Fed. Reg. 48458, 48482, n.334 (Aug. 10, 2010) (stating that while in rulemaking proceeding there was evidence that the collection of advance fees causes actual harm, the Section 5 unfairness standard does not require the Commission to "demonstrate *actual* consumer injury, but only the *likelihood* of substantial injury" (emphasis original)); *cf. Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at \*11-12 (7th Cir. July 20, 2015) (finding injury sufficient to satisfy Article III standing requirements because "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur" (quoting

*Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013)). Thus, that a practice, much less a sweeping set of practices as seen in this case, is likely to cause harm satisfies the unfairness analysis. *Int'l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*89 n.52 (1984) (rejecting dissent's assertion that the Commission was requiring actual harm rather than likelihood of harm, stating "[t]he ultimate question at issue is, indeed, risk. What is the risk of consumer harm?"); *see also id* at n.45 (noting that the reference to "risk" in the Unfairness Statement's discussion of an unfairness case involving health and safety risks "makes clear [that] unfairness cases may also be brought on the basis of likely rather than actual injury"). Failure to maintain adequate data security for Personal Information is likely to cause consumers substantial harm. CCCL ¶ 27.

That is especially the case here because, as described above, LabMD collected and stored on its computer network highly sensitive information about hundreds of thousands of consumers, including names and addresses, dates of birth, Social Security numbers, medical test codes, and health information. Sections 2.1.1 (LabMD's Collection and Maintenance of Consumers' Personal Information), 2.1.1.1 (LabMD's Collection and Maintenance of Consumers' Personal Information from Physician-Clients), 2.1.1.2 (LabMD's Collection and Maintenance of Consumers' Personal Information Directly from Consumers), *supra*. As previously detailed, LabMD provided unreasonable security for this extremely sensitive information through a series of actions and omissions. *See generally* Section 3, *supra*. These failures caused or are likely to cause substantial injury to the over 750,000 consumers whose Personal Information is maintained on LabMD's computer networks, including the nearly 10,000 consumers whose Personal Information was exposed in the 1718 File and the Sacramento Day Sheets and copied checks.



A practice is unfair if it causes or is likely to cause “a small amount of harm to a large number of people, or if it raises a significant risk of concrete harm.” *Int’l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*101 n.12 (1984) (Unfairness Statement).

LabMD’s failures placed the over 750,000 consumers whose Personal Information is maintained on LabMD’s computer networks, including the 9,300 consumers whose Personal Information was shared on a P2P network and the approximately 600 consumers whose Personal Information is contained in the Sacramento Day Sheets and copied checks, at risk of injury or harm,<sup>4</sup> including identity theft,<sup>5</sup> medical identity theft,<sup>6</sup> and medical identity fraud.<sup>7</sup> Sections 6.11 (LabMD’s Security Failures Placed All Consumers Whose Personal Information is On Their Network at Risk of Substantial Harm), 6.1.2 (Substantial Consumer Injury from Unauthorized Disclosure of 1718 File), 6.1.2.1 (Potential Identity Theft from Exposure of the 1718 File), 6.1.2.2 (Potential Medical Identity Theft from Exposure of the 1718 File), 6.1.2.1 (Reputational and Other Harms from Exposure of the 1718 File), 6.1.3 (Substantial Consumer Injury from Unauthorized Disclosure of the Sacramento Day Sheets and Copied Checks), *infra*. 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 harm and embarrassment. Section 6.1.3, *infra*. In exposing the Personal Information of 750,000

---

<sup>4</sup> “Injury” and “harm” are used interchangeably for purposes of this analysis.

<sup>5</sup> Identity theft, also referred to as identity fraud, is the unauthorized use of another’s personal information to achieve illicit financial gain. CCF ¶ 1475.

<sup>6</sup> 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. CCF ¶ 1483.

<sup>7</sup> Medical identity fraud is the unauthorized use of a third party’s personally identifiable information to obtain medical products or services, including but not limited to office visits and consultations, medical operations, and prescriptions. CCF ¶ 1484.

consumers to unauthorized disclosure, LabMD's data security failures are likely to cause injury to a large number of consumers.

The harm caused or likely to be caused by LabMD's failures are the types of harms that are cognizable under Section 5. Monetary harm exemplifies the injury prong of the unfairness standard. *Int'l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*97 (1984). Any consumers who suffer identity theft or medical identity theft as a result of LabMD's failures are likely to experience monetary harm. CCFF ¶¶ 1515, 1517-1518 (new account fraud), 1528-1529 (existing non-card fraud), 1539-1540 (existing card fraud), 1600-1603 (medical identity theft). Unfair acts or practices also cause substantial harm when consumers must spend "a considerable amount of time and resources" remediating problems caused by the conduct, such as closing compromised bank accounts. *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115-16 (S.D. Cal. 2008) (basing finding of substantial harm in part on "the cost of account holders' time" where defendants' practices compromised bank account security); *see also Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, 2015 U.S. App. LEXIS 12487 at \*9 (7<sup>th</sup> Cir. July 20, 2015) (observing in a data breach involving credit cards, "there are identifiable costs associated with the process of sorting things out"), \*13-14 (lost time and money spent by consumers protecting themselves from future identity theft "easily qualifies as a concrete injury"), \*21 (finding that mitigation expenses and future injury are judicially redressable); *FTC v. Kennedy*, 574 F. Supp. 2d 714, 721 (S.D. Tex. 2008) (finding substantial injury where, inter alia, "consumers were forced to expend substantial time and effort" seeking refunds and other remediation of the defendant's unfair conduct"). Any consumers who suffer identity theft or medical identity theft as a result of LabMD's failures are likely to spend many hours attempting

to resolve the fraud. CCFF ¶¶ 1521-1524 (new account fraud), 1532-1535 (existing non-card fraud), 1544 (existing card fraud), 1623-1624 (medical identity theft).

“Unwarranted health and safety risks may also support a finding of unfairness.” *Int’l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*97 (1984). Indeed, the seminal unfairness case involved a product that caused physical injury to some consumers and was likely to harm more. *Int’l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*90 & n.57 (1984). Consumers who are likely to experience medical identity theft due to LabMD’s failures may suffer physical harm from misdiagnoses or unnecessary treatments. CCFF ¶¶ 1612-1618. Further, LabMD’s failures led to the unauthorized disclosure of consumers’ sensitive medical information. CCFF ¶¶ 1363-1370, 1375-1376, 1393-1395 (1718 File); 1413-1414 (Sacramento Incident). Such a loss of privacy can result in a “host of emotional harms that are substantial and real and cannot fairly be classified as either trivial or speculative.” *FTC v Accusearch, Inc.*, 2007 WL 4356786 at \*8 (D. Wyo. Sept. 28, 2007). The disclosure of sensitive medical information, resulting in the loss of consumer privacy, constitutes substantial injury. CCCL ¶ 40.

#### **5.1.1 LabMD’s Security Failures Placed All Consumers Whose Personal Information is on Their Network at Risk of Substantial Harm**

LabMD’s failure to employ reasonable security measures placed all consumers whose Personal Information is on its network at risk. LabMD maintains Personal Information of over 750,000 consumers on its computer network, including: first and last name; telephone number; address; date of birth; Social Security number; medical record number; bank routing, account, and check numbers; credit or debit card information; laboratory test result, medical test code, or diagnosis, or clinical history; and health insurance company name and policy number. CCFF ¶¶ 89, 120, 134-138, 140-148. These items of Personal Information are the types of information

needed to perpetrate frauds, CCFE ¶ 1643, and are the target of data thieves. CCFE ¶ 1646-1650. The risk of unauthorized exposure of sensitive Personal information created by LabMD's failure to use reasonable measures to prevent unauthorized access to that information is likely to cause substantial harm to consumers in the form of identity theft, medical identity theft, and other harms. CCFE ¶¶ 1653-1658.

### **5.1.2 Substantial Consumer Injury from Unauthorized Disclosure of the 1718 File**

The exposure of the 1718 File on the Gnutella network is one example of how LabMD's security failures are likely to cause substantial harm to consumers. CCFE ¶¶ 1667-1671, 1675. 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. CCFE ¶ 1667. For example, in combination with a consumer's name, Social Security numbers can be used to gain direct access to financial accounts. CCFE ¶ 1489. Once a consumer's information is exposed, it is difficult for that consumer to detect and prevent misuse of his or her information. CCFE ¶ 1584. Further, certain types of Personal Information, such as Social Security numbers, rarely change and thus can be used fraudulently for extended periods of time; failure to reasonably secure these types of Personal Information is likely cause substantial injury indefinitely. CCFE ¶¶ 157-1575. This demonstrates that risk of substantial harm is ongoing and will continue into the future. 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; the failure to secure the 1718 File is likely to cause them substantial injury. CCFE ¶ 1668.

### 5.1.2.1 Potential Identity Theft from Exposure of the 1718 File

Consumers whose Personal Information was contained in the 1718 File are likely to experience substantial harm by having their information used by identity thieves because the file was shared on the Gnutella network where any Gnutella user could access it. CCFE ¶¶ 1363-1370, 1375-1377. LabMD's failure to provide reasonable security for the types of information in the 1718 File places consumers at a significantly higher risk of becoming a victim of identity theft, and is thus likely to cause them substantial harm. CCFE ¶¶ 1667-1671.

Consumers whose Personal Information was compromised in a data breach are significantly more likely to suffer identity fraud than consumers whose Personal Information was not compromised, indicating that failure to secure the information is likely to cause substantial harm. CCFE ¶¶ 1506-1512. In 2013, while only 2.7% of all Americans who were not notified that their information was compromised in a data breach in the last 12 months reported becoming a victim of identity fraud in the last 12 months, 30.5% of data breach victims had also fallen victim to identity fraud. CCFE ¶¶ 1507-1508. Consumers affected by an unauthorized disclosure of their Personal Information are likely to suffer substantial harm as result of fraud, such as existing card fraud,<sup>8</sup> existing non-card fraud,<sup>9</sup> and new account fraud.<sup>10</sup> CCFE ¶ 1515. These types of fraud result in financial harm to consumers as well as requiring consumers to

---

<sup>8</sup> Existing card fraud is identity theft perpetrated through the use of existing credit or debit cards and/or their account numbers. CCFE ¶ 1480.

<sup>9</sup> Existing non-card fraud is identity theft perpetrated through the use of existing checking or savings accounts of existing loans, insurance, telephone and utilities accounts, along with income tax fraud and medical identity fraud. CCFE ¶ 1481.

<sup>10</sup> 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. CCFE ¶ 1482.

spend time to resolve the fraud. CCFE ¶¶ 1517-1518, 1521-1525, 1528-1529, 1532-1536, 1539-1541, 1544.

#### **5.1.2.2 Potential Medical Identity Theft From Exposure of the 1718 File**

The exposure of consumers' medical information contained on LabMD's system caused or is likely to cause substantial injury to consumers in the form of medical identity theft, as exemplified by the exposure of the 1718 File on the Gnutella network. CCFE ¶ 1668, 1678-1681. Medical identity theft can damage a consumer's economic well-being and reputation, and even risk his or her health. CCFE ¶¶ 1600-1603, 1606-1609, 1612-1618, 1621. 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. CCFE ¶¶ 1600-1603, 1606-1609, 1612-1618, 1621.

Over one third of medical identity theft victims incur an average of \$18,660 in out-of-pocket expenses. CCFE ¶ 1602. Those costs include: (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. CCFE ¶ 1603.

In addition to suffering financial harm from medical identity theft, consumers whose Personal Information is used by identity thieves are also likely to experience adverse health consequences. CCFE ¶¶ 1612-1618. For example, one study found that 15% of medical identity theft victims had a misdiagnosis of illness, 14% had a delay in receiving medical treatment, 13% had a mistreatment of illness, and 11% had wrong pharmaceuticals prescribed. CCFE ¶ 1616. Direct physical harm could occur, for example, when a change is made to a consumer's medical record that could result in improper or unnecessary treatments. CCFE ¶ 1617. When a

consumer's electronic health record is compromised and the health information of the identity thief merges with that of the consumer, the resulting inaccuracies could pose a serious risk to the health and safety of the consumer by, for instance, associating the wrong blood type with the victim or obscuring life-threatening drug allergy information. CCFE ¶ 1613.

### **5.1.2.3 Reputational and Other Harms from Exposure of the 1718 File**

Failure to secure Personal Information, such as that found in the 1718 File, is also likely to cause consumers substantial reputational and other privacy harms. The 1718 File includes current procedural terminology (CPT) codes, some of which indicate tests for sensitive conditions. CCFE ¶¶ 1685-1686. For example, some of the CPT codes in the 1718 File indicate tests for prostate cancer, testosterone levels, and sexually transmitted diseases, specifically HIV, hepatitis, and herpes. CCFE ¶¶ 1686, 1688-1692. 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. CCFE ¶¶ 1687, 1696-1697. Moreover, once health information is disclosed, it is impossible to restore a consumer's privacy. CCFE ¶¶ 1700-1701.

### **5.1.3 Substantial Consumer Injury From Unauthorized Disclosure of the Sacramento Day Sheets and Copied Checks**

The unauthorized disclosure of the Sacramento Day Sheets and copied checks caused or is likely to cause substantial injury to consumers. CCFE ¶¶ 1714-1719, 1722-1733, 1736-1739, 1742-1746, 1749-1753, 1756-1760. The Day Sheets and copied checks contain sensitive Personal Information, including first names and last names, middle initials, and Social Security numbers for approximately 600 consumers, and bank routing and account numbers for consumers whose checks are included. CCFE ¶¶ 1714-1717, 1723. These types of information can be used by identity thieves to commit identity theft resulting in monetary and other harms to

affected consumers. CCFE ¶ 1487-1493. Because consumers rarely change their Social Security numbers, they can be fraudulently used for extended periods of time, making it likely that consumers will suffer injury. CCFE ¶¶ 1570-1575. The fact that the Day Sheets and copied checks were found, with other evidence of identity theft, in the possession of known identity thieves speaks to the value of the consumer information in the documents and the likelihood that it may have been misused. CCFE ¶¶ 1727-1729.

Consumers will incur an estimated \$36,277 in out of pocket costs from fraud resulting from 164 cases of new account fraud, existing non-card fraud, and existing card fraud due to the unauthorized disclosure of the Day Sheets. CCFE ¶¶ 1736-1739, 1742-1746, 1749-1753, 1756-1760. Consumers will also spend an anticipated 2,497 hours resolving fraud arising from the disclosure of their sensitive information in the Day Sheets. CCFE ¶ 1739.

## **5.2 The Harm Caused or Likely to Be Caused By LabMD's Failures is Not Reasonably Avoidable by Consumers Themselves**

Consumers cannot reasonably avoid the substantial harm caused or likely to be caused by LabMD's continuing failure to employ reasonable security measures for the Personal Information maintained on its computer network. The unauthorized disclosures of the 1718 File and the Sacramento Day Sheets and checks provide ample evidence of the likelihood of this harm. A consumer is not in a position to know about the security practices of every company that maintains his or her information. CCFE ¶¶ 1773-1774. Where consumers do not have a free and informed choice, injury is not reasonably avoidable. *Davis v. HSBC Bank Nevada, N.A.*, 691 F.3d 1152, 1168-69 (9th Cir. 2012); *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1158 (9th Cir. 2010). An injury is reasonably avoidable if consumers "have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end." *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365



(11th Cir. 1988) (quoting *In re Orkin Exterminating Co.*, 108 F.T.C. 341, 366 (1986)). In most instances, consumers needing medical tests would not know LabMD would test their specimen and receive their Personal Information. CCFE ¶¶ 1777-1782. Consumers could not therefore have known what LabMD's security practices were before their specimens were sent to LabMD. CCFE ¶¶ 1785-1787. Additionally, LabMD maintains sensitive personal data of approximately 100,000 consumers who never had tests conducted by LabMD. CCFE ¶¶ 78-79. These consumers have no relationship with the company and likely never had notice that their data was provided to it. *See* CCFE ¶¶ 1777-1782. Therefore, consumers cannot reasonably avoid the harm caused or likely to be caused by LabMD's failure to provide reasonable security for their Personal Information maintained on its computer network.

### **5.3 The Harm Caused or Likely to be Caused by LabMD's Failures is Not Outweighed by Countervailing Benefits to Consumers or Competition**

The harms likely to be caused by LabMD's data security failures are not outweighed by countervailing benefits to consumers or competition. *See generally* CCCL ¶¶ 46-53. “[W]hen a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition,” the countervailing benefits prong of the unfairness test is “easily satisfied.” *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (quoting *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal 2000)). Countervailing benefits are determined based on the specific practice at issue in a complaint, not the overall operation of a business. *See FTC v. Accusearch, Inc.*, 2007 WL 4356786, at \*8 (D. Wyo. Sept. 28, 2007), judgment aff'd *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988); *Apple, Inc.*, No. 122-3108, Statement of Comm'r Maureen K. Ohlhausen at 2 (Jan. 15, 2014). Because LabMD's data security failures could have been detected and corrected at low or no

cost, LabMD's data security failures did not provide any advantage over competing laboratories, and provided no countervailing benefit to consumers or competition. *See FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008); *Int'l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290, at \*90 (F.T.C. Dec. 21, 1984).

LabMD engaged in a number of practices that failed to adequately prevent or detect unauthorized access to personal information even though it could have corrected the failures at low cost. For example, because LabMD did not require hard-to-guess passwords for authentication, intruders could easily guess passwords and then use them to impersonate employees to access employee computers and sensitive information stored on them. CCFE ¶¶ 909-951. And, as noted above, LabMD could have obtained an intrusion detection system at no cost. *Supra* Section 2.3.2 (LabMD Did Not Implement Automated Scanning Tools). By failing to use low cost monitoring tools such as Wireshark, LabMD denied itself the opportunity to detect unauthorized transfers of sensitive information from its network, CCFE ¶¶ 651-657, 1129-1131, such as might occur through a successful password guessing attack, CCFE ¶¶ 909-916. It could have implemented software tools that it had already purchased—such as a password management system, CCFE ¶¶ 1165-1167; an access control system, CCFE ¶¶ 1149-1151; and a software firewall, CCFE ¶ 1131—at no cost. It also could have subscribed to vulnerability reporting systems, CCFE ¶ 1134, provided free security training to its IT employees, CCFE ¶¶ 1157-1162, and used widely-available security policy templates, CCFE ¶¶ 1121-1124, at no cost.

By failing to use file integrity monitor products, even though it could have done so at very low cost, LabMD could not detect changes in critical files to investigate whether they were caused by unauthorized programs or malware. CCFE ¶¶ 514-521, 705-712, 1108-1110, 1136,

1184. Finally, by failing to effectively enforce the software monitoring policy it claims it followed starting in 2002, LabMD also failed to detect and remove the LimeWire program the billing manager used to make the 1718 File available to others on P2P networks. CCFF ¶¶ 465-471.

Other measures would have greater, but still low, costs. For instance, periodically purging unnecessary data, training non-IT employees, and reviewing antivirus scans would have required some employee time. CCFF ¶¶ 1152-1162. Similarly, upgrading its Windows operating systems would have incurred cost. But by failing to do so, LabMD kept open paths that could be used to obtain unauthorized access to its network and the sensitive information on it. CCFF ¶¶ 996-1008. Given the highly-sensitive nature of the data LabMD collected and the likelihood of harm unauthorized exposure of that data would cause to consumers, any costs to LabMD of improving its security are far outweighed by the benefits to consumers of having their data adequately protected.

Taken together, LabMD's unreasonable data security practices caused or are likely to cause substantial harm to hundreds of thousands of consumers. Because LabMD could have corrected most of the failures using its own employees and available tools, its inadequate security practices failed to provide any countervailing benefits to consumers or competition (such as lower prices to consumers or insurers). *See FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008); *Int'l Harvester Co.*, Docket No. 9147, 104 FTC 949, 1984 WL 565290 at \*90 (1984).

**6. COMPLAINT COUNSEL'S PROPOSED ORDER IS APPROPRIATE AND SHOULD BE ENTERED**

Complaint Counsel respectfully requests that the Court enter the proposed Notice Order accompanying the Complaint, as revised by the attached proposed Notice Order.<sup>11</sup> While LabMD has suspended its acceptance of consumer patient specimens at present, it has no intent to dissolve as a Georgia corporation, retains the Personal Information of over 750,000 consumers, and continues to operate a computer network. CCCL ¶¶ 57-71. These facts demonstrate that “there exists some cognizable danger of recurrent violation,” and entry of an order containing injunctive provisions is appropriate. *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1201 (10th Cir. 2009) (citing *U.S. v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953)); see also *FTC v. Commerce Planet, Inc.*, 878 F. Supp. 2d 1048, 1087-88 (C.D. Cal. 2012) (finding permanent injunction appropriate where defendant continued to work in same business field, even though no longer involved in the same type of conduct); *FTC v. RCA Credit Services, LLC*, 727 F. Supp. 2d 1320, 1337 (M.D. Fla. 2010) (finding that defendant’s new business venture in a similar industry “present significant opportunities for similar violations”); *FTC v. Bronson Partners, LLC*, 674 F. Supp. 2d 373, 393-94 (D. Conn. 2009) (imposing a permanent injunction where discontinued conduct was “obvious and widespread” rather than “a single instance”). The Notice Order is essential to protect consumers, as LabMD intends to apply the same data security policies and procedures to information in its possession as it has employed in the past. CCCL ¶¶ 61, 69-71. Furthermore, the discovery of the sensitive Personal Information of over six hundred consumers in the hands of confessed identity thieves in Sacramento, California in 2012 indicates that the

---

<sup>11</sup> The attached proposed Notice Order differs only in that it excludes from the definition of “Affected Consumers,” for purposes of direct notification to consumers, those consumers included in the Day Sheets and cancelled checks found in the Sacramento incident to whom LabMD has previously provided notice.

exposure of sensitive data from LabMD's files was not a one-time occurrence. See CCCF ¶¶ 1413-1414 (Sacramento incident). While there is no conclusive explanation of how that data was exposed, the fact that it was discovered in identity thieves' possession in 2012 demonstrates that leaks of LabMD's sensitive data and the resulting consumer injury are ongoing concerns. CCCF ¶ 1413-1414, 1433-1444. Entry of the Notice Order is the only thing standing between consumers and identity theft.

### 6.1 Fencing-In Relief is Appropriate

As the Supreme Court described in the *Ruberoid* case, the Commission has "wide discretion" in crafting an appropriate remedy against FTC Act violators. *FTC v. Ruberoid Co.*, 343 U.S. 470, 473 (1952); see also *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 611-13 (1946). The Court and the Commission consider the appropriateness of fencing-in relief by examining the deliberateness and seriousness of the violations; the degree of transferability of unlawful conduct to other products; and whether the respondent has a history of past violations. *Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6, at \*414-15 (1984); *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992). Another court identified: "the egregiousness of the defendant's actions, the isolated or recurrent nature of the infraction, the degree of scienter involved, the sincerity of the defendant's assurances against future violations, the defendant's recognition of the wrongful nature of his conduct, and the likelihood that the defendant's occupation will present opportunities for future violations." *FTC v. Direct Mktng. Concepts, Inc.*, 648 F. Supp. 2d 202, 212 (D. Mass. 2009) (citing *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1017 (N.D. Ind. 2000)). However phrased, the factors warrant an injunction in this matter.

Fencing-in provisions are appropriate where they are "reasonably related" to the conduct at issue. *FTC v. Direct Mktng. Concepts, Inc.*, 648 F. Supp. 2d 202, 216 (D. Mass. 2009).

“The reasonable relationship analysis operates on a sliding scale – any one factor’s importance varies depending on the extent to which the others are found. . . . All three factors need not be present for a reasonable relationship to exist.” *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 309 (May 17, 2012) (quoting *Telebrands Corp.*, 457 F.3d at 358-59). The more egregious the facts with respect to a particular element, the less important it is that another negative factor be present. *See Sears, Roebuck & Co.*, 676 F.2d 385, 392 (9th Cir. 1982); *Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6, at \*414 (1984).

Respondent’s data security failures were deliberate. LabMD had control over and made decisions regarding its data security practices. CCCL ¶¶ 91-103. LabMD failed to adopt and implement reasonable data security policies, CCFF ¶¶ 397-455, and even where it had policies for data security in place, it often violated or failed to fully implement the policies, CCFF ¶¶ 458-480. Respondent also failed to remediate security risks that were brought to its attention. For example, it did not fix issues identified in scans conducted by a third party—even where the third party identified the solution. CCFF ¶¶ 759-771 (vulnerability identified in May 2010 scan still present in July 2010); CCFF ¶¶ 781-789 (vulnerability identified in May 2010 scan still present in July 2010); CCFF ¶¶ 792-797 (vulnerability identified in May 2010 scan still present in September 2010). It also failed to update its antivirus software for several months even after it was informed that the software was no longer supported. CCFF ¶¶ 539-550.

LabMD’s data security failures are pervasive and persistent, rather than isolated, involving multiple types of problems over many years. *See generally* CCFF ¶¶ 382-1110 (§ 5). These deliberate actions indicate scienter. LabMD, through its employees and contractors, made decisions regarding data security, such as failing to enforce its security policies, CCFF ¶¶ 458-480; failing to consistently run and review antivirus scans, CCFF ¶¶ 527-629; haphazardly

deploying incomplete and ineffective manual inspections, CCFE ¶¶ 660-696; and permitting employees to use weak passwords for years, CCFE ¶¶ 903-993. LabMD's failure to take responsibility for its lax data security, its plan to maintain the same unreasonable security practices in the future, and its refusal to acknowledge its data security issues also demonstrate the deliberateness of its actions and the need for injunctive relief. *Compare, e.g.*, LabMD's Motion to Admit RX-543 – RX-548 at 6 (asserting that Complaint Counsel should have investigated Tiversa rather than LabMD in connection with the release of the 1718 File), *with* JX0001-A (Joint Stips. of Law and Fact) at 4 (stipulating that LimeWire was installed on the billing manager's computer and that 900 files, including the 1718 File, were designated for sharing). LabMD retains the Personal Information of 750,000 consumers, which continues to be at risk.

LabMD's data security failures were serious. The seriousness of the violations in this case is illustrated by the types of Personal Information LabMD holds, which are among the most sensitive pieces of Personal Information, CCFE ¶¶ 1642-1650, and the harm likely to be caused to consumers, including identity theft, medical identity theft, and other harms, by breach of this Personal Information. *See generally* CCFE ¶¶ 1642-1658. The seriousness of the violations is also illustrated by the duration of LabMD's data security failures. *See* CCCL ¶¶ 105-110; *Kraft v. FTC*, 970 F.2d 311, 326 (7th Cir. 1992) (finding a violation serious due to, inter alia, its two and one-half year duration). The inability of consumers to protect themselves from the risks LabMD's failures posed to their Personal Information is another indicium of seriousness. *See Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 312 (May 17, 2012) (finding violation serious where consumers did not have to ability to evaluate health claims made in advertisement); *Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6, at \*417 (1984); CCFE ¶¶ 1773-1795. The seriousness of the violations in this case is further

highlighted by the exposure of the 1718 File and the Day Sheets. CCF § 1354-1469 (Security Incidents at LabMD).

LabMD's conduct with respect to its data security failures is transferable, not only in continuing to endanger the Personal Information of the 750,000 consumers that it already holds, but also affecting any additional consumers to whom it provides services in the future. There are no steps that consumers can themselves take to protect their Personal Information that LabMD currently holds and prevent future harm. Consumers did not know, in most cases, that their Personal Information was sent to LabMD, nor did they know its security practices, CCF § 1777-1787, and even if they did have such knowledge, notice does not allow for full remediation of the dangers of identity theft and fraud. CCF § 1769-1770.

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



While there are no previously adjudicated findings of Section 5 violations against LabMD, where the conduct is sufficiently deliberate and serious as to establish a reasonable relationship between the remedy and the violation, this factor is not necessary to the appropriateness of fencing-in relief in an order. *Telebrands Corp. v. FTC.*, 457 F.3d 354, 362 (4th Cir. 2006); *Kraft v. FTC*, 970 F.2d 311, 327 (7th Cir. 1992) (concluding claim that fencing-in provision was inappropriate because of a lack of prior violations “without merit”); *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012). “The more egregious the facts with respect to a particular element, the less important it is that another negative factor be present. In the final analysis, we look to the circumstances as a whole and not to the presence or absence of any single factor.” *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 392 (9th Cir. 1982).

Thus, fencing-in relief is not only appropriate, but essential in this case where the violations are serious, deliberate, and readily transferable. *See, e.g., Brake Guard Prods., Inc.*, 125 F.T.C. 138, 253-254 (1998) (misrepresentations related to motor vehicle safety were serious); *Schering Corp.*, 118 F.T.C 1030, 1121 (1994) (Initial Decision) (violations were serious where claims consciously made despite flaws in the studies respondent relied on and because consumers were not able to assess the validity of the claims); *Thompson Med. Co.*, Docket No. 9149, 104 F.T.C. 648, 1984 FTC LEXIS 6, at \*414-16 (1984) (long-term, deliberate, transferrable violations warrant fencing-in relief).<sup>12</sup>

---

<sup>12</sup> The term “fencing in” is not limited to advertising cases and describes prophylactic order provisions in general. *See, e.g., FTC v. Nat’l Lead Co.*, 352 U.S. 419, 431 (1957).

## 6.2 The Notice Order is Reasonably Related to LabMD's Unlawful Practices and is Clear and Precise

Whether the case involves consumer protection or competition violations, the “wide discretion” in crafting an appropriate order described in *Ruberoid* is subject only to two constraints: the order must bear a “reasonable relation” to the unlawful practices, *Jacob Siegel Co.*, 327 U.S. at 612-13, and it must be sufficiently clear and precise that its requirements can be understood, *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 392 (1965). Pursuant to this authority, the courts have affirmed Commission orders requiring remedies in diverse factual scenarios. *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 431 (1957) (limiting individual use of zone pricing); *N. Tex. Specialty Physicians v. FTC*, 528 F.3d 346, 372 (5th Cir. 2008) (requiring cancellation of existing contracts); *Chicago Bridge & Iron Co. N.V. v. FTC*, 534 F.3d 410, 441 (5th Cir. 2008) (mandating divestiture of assets to create a competitor); *Sears, Roebuck & Co. v. FTC*, 676 F.2d 385, 389 n.10, 400 (9th Cir. 1982) (requiring competent and reliable evidence for future performance claims for major household appliances); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192, 197 (D.C. Cir. 1986) (requiring at least two adequate and well-controlled, double-blinded clinical studies for future efficacy claims for a topical analgesic); *Porter & Dietsch, Inc. v. FTC*, 605 F.2d 294, 306-07 (7th Cir. 1979) (mandating disclosure requirements); *Cont'l Wax Co. v. FTC*, 330 F.2d 475, 479-80 (2d Cir. 1964) (requiring trade name excision). In each instance, the underlying inquiry has been the same: what remedy is needed to ensure that respondents do not again violate the FTC Act. See *Colgate-Palmolive Co.*, 380 U.S. at 394-95 (noting that the Commission may frame its order broadly enough to prevent respondents from engaging in similar illegal practices).

The Notice Order issued by the Commission contains three provisions designed to prevent future violations by LabMD and to remediate, to the extent possible, the risk of

likelihood of harm to which it has exposed consumers. Parts I and III arise directly from the conduct alleged in Complaint Counsel's Complaint, while Part II is a fencing-in provision requiring the use of a third party to examine and certify the sufficiency of LabMD's data security program. The Notice Order's twenty year order duration is consistent with the Commission's prior orders, *see, e.g., Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012); *Daniel Chapter One*, 2010 FTC LEXIS 11, at \*9-10 (2010), and is appropriate given the length of time over which LabMD's unreasonable data security practices extended. CCCL ¶¶ 116-120; *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 325 (May 17, 2012) (finding 20 year order duration appropriate where advertisements were disseminated over course of several years).

Part I of the Notice Order requires LabMD to establish, implement, and maintain a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of Personal Information collected from or about consumers. The program must be in writing, and should contain administrative, technical, and physical safeguards appropriate to LabMD's size and complexity, the nature and scope of its activities, and the sensitivity of the Personal Information collected from or about consumers. This provision is consistent with relief approved in Commission settlements relating to unfair data security practices. *See, e.g., CCCL* ¶¶ 19-20; *see also U.S. v. Consumer Portfolio Services, Inc.*, Case No. 8:14-cv-00819-ABC-RNB at 6-7, Section IV (Stipulated Order for Perm. Injunct.) (C.D. Cal. June 11, 2014), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc> (requiring debt collector to implement a comprehensive data integrity program with elements similar to a comprehensive data security program), as well as the Commission's Safeguards Rule of the Gramm-Leach Bliley Act, 16 C.F.R. § 314.4. The

Commission has provided a large amount of guidance to businesses for complying with the Safeguards Rule and on general data security practices. *See, e.g.*, Financial Institutions and Customer Information: Complying with the Safeguards Rule, *available at* <http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule>; Protecting Personal Information: A Guide for Business, *available at* <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>; *see generally* FTC Bureau of Consumer Protection Business Center: Data Security, *available at* <http://business.ftc.gov/privacy-and-security/data-security>. Other sources, such as NIST, SANS, and US CERT, have provided guidance for implementing a comprehensive information security program. Given this extensive guidance, the provision is sufficiently clear and precise that its requirements can be understood. *See Colgate-Palmolive Co.*, 380 U.S. at 392.

Part II of the Notice Order requires LabMD to obtain initial and then biennial assessments and reports for twenty years from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The Notice Order provides examples of the types of qualifications that are sufficient for such third-party professionals. The provision is consistent with prior Commission orders in data security cases, *see, e.g.*, CCCL ¶¶ 19-20, and enumerates the elements that must be included in the assessment, which must: (1) set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained; (2) explain how the safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Personal Information collected from or about consumers; (3) explain how the safeguards that have been implemented meet or exceed the provisions in Part I of the order; and (4) certify that respondent's security program provides reasonable assurance that the

security, confidentiality, and integrity of Personal Information is protected. Such independent third-party review is appropriate fencing-in relief, which often relies on third party verification of a respondent's conduct and compliance with an order. CCCL ¶ 133-136.

A fencing-in provision must bear a "reasonable relation" to the unlawful practices, *Jacob Siegel Co.*, 327 U.S. at 612-13; and it must be sufficiently clear and precise that its requirements can be understood, *Colgate-Palmolive Co.*, 380 U.S. at 392. Part II of the Notice Order meets these requirements. Part II is reasonably related to LabMD's conduct. For example, even where the company had data security policies, it did not adequately enforce them, or provide the tools needed to implement them. CCFE ¶¶ 458-480. The four provisions of the fencing-in relief laid out in Part II, along with the necessary credentials of the third party, are clear and precise, particularly given that a virtually identical provision has been imposed in many of the Commission's past orders. CCCL ¶¶ 12-22.

Part III of the Notice Order requires LabMD to notify Affected Individuals in the 1718 File regarding the unauthorized disclosure of their Personal Information, as well as the insurance companies for Affected Individuals in the 1718 File and the Sacramento documents.<sup>13</sup> Notice to affected consumers is an appropriate remedy. *Int'l Harvester Co.*, 1984 WL 565290, at \*94 (noting that an order requiring disclosure of a hazard to consumers "is our ordinary and presumptive response" that is appropriate "even when the respondent has ceased engaging in the conduct in question"); *see also FTC v Accusearch, Inc.*, 2007 WL 4356786, at \*9 (D. Wyo. Sept. 28, 2007) (entering order requiring consumer notice as a remedy where defendant's had unfairly procured the consumers' phone records); *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-

---

<sup>13</sup> LabMD previously provided notice to consumers in the Sacramento documents, CCFE ¶¶ 1462-1470, but did not notify those consumers' insurance providers.

01830 at 7, Section IV (Stip. Prelim. Injunct.) (D.D.C. Nov. 3, 2014), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/142-3226/bayview-solutions-llc> (requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *FTC v. Cornerstone & Co., LLC*, Case No. 1:14-CV-01479, at 7, Section IV (Stip. Prelim. Injunct.) (D.D.C. Sept. 10, 2014), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/142-3211/cornerstone-company-llc> (requiring notice to consumers whose Personal Information defendants disclosed without implementing and using reasonable safeguards to maintain and protect the privacy, security, confidentiality, and integrity of the information); *Warner-Lambert Co. v. FTC*, 562 F.2d 749, 762 (D.C. Cir. 1977) (corrective advertising is an appropriate remedy); *Wasem 's, Inc.*, Docket No. C-2524, 1974 FTC LEXIS 134, at \*11 (July 23, 1974) (consent order) (requiring respondent to devote 25% of its advertising time to corrective advertising to counteract previous erroneous and misleading advertising claims). Without notification, consumers have no way of independently knowing about an organization's unauthorized disclosure of their sensitive information, nor that they should take actions to reduce their risk of harm from identity crime. CCF ¶¶ 1708-1711.

Likewise, notice to Affected Consumers' insurance companies is an appropriate remedy, to provide them with an opportunity to protect consumers' identity from misuse. Third party notices are a commonly used remedy to mitigate harms. *See, e.g., PPG Architectural Finishes, Inc.*, Docket No. C-4385, 2013 FTC LEXIS 22, at \*8-9, 13-14 (Mar. 5, 2013) (consent order) (notices sent to dealers, distributors, and other entities to stop using prior advertising materials with deceptive no VOCs claim for paint and to apply the enclosed stickers to product labeling); *Oreck Corp.*, 151 F.T.C. 289, 371-72, 376-77 (May 19, 2011) (consent order) (notice sent to

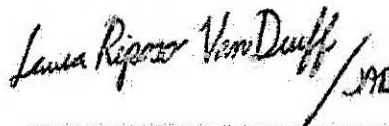
franchisees); *Indoor Tanning Ass'n.*, 149 F.T.C. 1406, 1439, 1443-44 (May 13, 2010) (consent order) (notices sent to association members and other prior recipients of point-of-sale materials); *Cytodyne LLC*, 140 F.T.C. 191, 209, 214-15 (Aug. 23, 2005) (consent order) (notices sent to purchaser for resale of weight-loss supplement); *Snore Formula, Inc.*, 136 F.T.C. 214, 298-99, 304-05 (July 24, 2003) (consent order) (notices sent to distributors who had purchased the product from the respondents or one of the respondents' other distributors); *MaxCell BioScience, Inc.*, 132 F.T.C. 1, 58-59, 66-67 (July 30, 2001) (consent order) (notice to distributors); *Alternative Cigarettes, Inc.*, No. C-3956, 2000 FTC LEXIS 59, at \*24, 31-33 (Apr. 27, 2000) (consent order) (notices to retailers, distributors, or other purchasers for resale to which respondents supplied cigarettes); *Body Sys. Tech., Inc.*, 128 F.T.C. 299, 312, 318-19 (Sept. 7, 1999) (consent order) (notice to distributors); *Brake Guard Prods., Inc.*, 125 F.T.C. 138, 259-60, 263-64 (Jan. 15, 1998) (notice to resellers); *Phaseout of Am., Inc.*, 123 F.T.C. 395, 457, 461-63 (Feb. 12, 1997) (consent order) (notice to resellers); *Consumer Direct, Inc.*, No. 9236, 1990 FTC LEXIS 260, at \*10-11, 20-21 (May 1, 1990) (consent order) (notice to credit card syndicators); *Third Option Labs., Inc.*, 120 F.T.C. 973, 996, 1001 (Nov. 29, 1995) (consent order) (notice to resellers); *Canandaigua Wine Co.*, 114 F.T.C. 349, 359-60 (June 26, 1991) (consent order) (notice to distributors and retailers).

The remaining Order provisions are standard. One of the purposes of injunctive relief is “monitoring compliance with the law and the terms of the injunction.” *Direct Mktng. Concepts, Inc.*, 648 F. Supp. 2d at 212. Monitoring provisions to ensure compliance with injunctions are appropriate to include in FTC orders. *FTC v. RCA Credit Svcs, LLC*, 727 F. Supp. 2d 1320, 1335 (M.D. Fla. 2010). The recordkeeping provisions in Parts IV-VIII of the Notice Order are consistent with those in other FTC orders. *See, e.g.*, cases cited in CCCL ¶ 19; *Pom Wonderful*

LLC, Docket No. 9344, Initial Decision at 325 (May 17, 2012). Part IV is a record-keeping requirement. Part V sets forth Order distribution requirements. Part VI requires LabMD to file notifications about changes in corporate structure. Part VII sets forth compliance reporting requirements. Finally, Part VIII is a sunset provision.

Dated: August 12, 2015

Respectfully submitted,

Handwritten signature of Laura Riposo VanDruff in black ink, with the initials 'LRB' written at the end of the signature.

---

Alain Sheer  
Laura Riposo VanDruff  
Megan Cox  
Ryan Mehm  
Jarad Brown

Federal Trade Commission  
600 Pennsylvania Ave., NW  
Room CC-8232  
Washington, DC 20580  
Telephone: (202) 326-2999  
Facsimile: (202) 326-3062  
Electronic mail: [lvandruff@ftc.gov](mailto:lvandruff@ftc.gov)

*Complaint Counsel*



**CERTIFICATE OF SERVICE**

I hereby certify that on August 12, 2015, I caused the foregoing document to be filed electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

I also certify that I caused a copy of the foregoing document to be transmitted *via* electronic mail and four hard copies delivered 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:

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


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

**CERTIFICATE FOR ELECTRONIC FILING**

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

August 12, 2015

By: \_\_\_\_\_

  
Jarad Brown  
Federal Trade Commission  
Bureau of Consumer Protection

# Attachment 1

**ORDER**

**DEFINITIONS**

For purposes of this order, the following definitions shall apply:

1. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
2. Unless otherwise specified, "respondent" shall mean LabMD, Inc., and its successors and assigns.
3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents, but for purposes of Parts III.A and III.C of this Order excluding consumers listed in the Sacramento Documents to whom LabMD has already provided notice of the breach.
4. "Insurance File" shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network.
5. "Personal information" shall mean 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.
6. "Sacramento Documents" shall mean the documents identified in Appendix A to Complaint Counsel's Complaint filed August 28, 2013.

**I.**

**IT IS ORDERED** that the respondent shall, no later than the date of service of this order, establish and implement, and thereafter 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 by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and

complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program;
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

## II.

**IT IS FURTHER ORDERED** that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days

after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099. Provided, however, that in lieu of overnight courier, assessments may be sent by first-class mail, but only if an electronic version of any such assessment is contemporaneously sent to the Commission at [Debrief@ftc.gov](mailto:Debrief@ftc.gov).

### III.

**IT IS FURTHER ORDERED** that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of service of this order unless an appropriate notice has already been provided, as follows:

- A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:
  - 1. a brief description of why the notice is being sent, including the

approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.), and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website ([www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com) and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and
  3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.
- B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.
- C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

#### IV.

**IT IS FURTHER ORDERED** that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and
- B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

## V.

**IT IS FURTHER ORDERED** that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

## VI.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at [Debrief@ftc.gov](mailto:Debrief@ftc.gov).

## VII.

**IT IS FURTHER ORDERED** that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to [Debrief@ftc.gov](mailto:Debrief@ftc.gov) or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099.



VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in less than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.