UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Terrell McSweeny

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

COMPLAINT COUNSEL'S CORRECTED* APPEAL 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's Corrected Appeal Brief corrects errors in the Table of Authorities contained in Complaint Counsel's Appeal Brief filed December 22, 2015. Besides those corrections, this document is identical to Complaint Counsel's Appeal Brief.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Legislative History

Cases

Regulations

Administrative Materials

Rules

RECORD REFERENCE ABBREVIATIONS

CCFF – Complaint Counsel's Proposed Findings of Fact

CCPTB – Complaint Counsel's Post-Trial Brief

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

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

CX0000 – Complaint Counsel's Exhibit

CX0000 (Witness, Dep.) at xx – Citations to Deposition Testimony

CX0000 (Witness, IHT) at xx – Citations to Investigational Hearing Testimony

ID – Initial Decision

Witness, Tr. 0000 – Citations to Trial Testimony

I. INTRODUCTION

LabMD is a multi-million dollar medical testing company that maintains the names, addresses, dates of birth, Social Security numbers, medical diagnoses, financial account information, health insurance information, and financial account information of 750,000 consumers. Despite maintaining consumers' most sensitive personal information, LabMD did not take even the most basic steps to secure it from those who had no right to see it, both within and outside LabMD. LabMD's pervasive security failures caused or were 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 against unfair practices. 15 U.S.C. § 45(a)(l). The Initial Decision's holding – that Complaint Counsel did not meet its burden of proving that LabMD's practices caused or were likely to cause substantial consumer injury – is in error. Complaint Counsel respectfully requests that the Commission reverse the Initial Decision, review the record *de novo*,[1] find that LabMD violated Section 5 of the FTC Act, and enter the notice order attached.

II. SUMMARY OF FACTS

LabMD conducts laboratory tests on specimen samples from consumers throughout the United States and reports test results to physicians. ID at18-19, ¶¶ 26-29. From January 1, 2005 through February 10, 2014, LabMD's total revenue was approximately $35 to $40 million.

---

[1] This brief addresses the Initial Decision, which analyzed only the first prong of Section 5(n)'s Unfairness Test. In addition to proving that LabMD's data security failures harmed consumers, as discussed throughout this brief, Complaint Counsel also proved that consumers could not reasonably avoid the harm that LabMD caused them, CCPTB at 72-73, and that the harm was not offset by countervailing benefits to consumers or competition. CCPTB at 73-75.

CCFF ¶¶ 57-61. In the course of its business, LabMD collected and retains the personal information of over 750,000 consumers. ID at 20, ¶ 42.

LabMD's business is predicated on collecting and maintaining on its computer network and on paper the most sensitive categories of consumers' personal information, including names, addresses, dates of birth, Social Security numbers, medical diagnoses, health insurance information, and financial information, such as credit card and bank account numbers. CCFF ¶¶ 12, 71; ID at 20, 22, ¶¶ 44, 58-62. The need for security is heightened when a company collects such sensitive information. CCFF ¶ 392. Here, LabMD failed to maintain reasonable security, particularly in light of the large volume of highly sensitive personal information it collected and maintains.

LabMD's failures were multiple, systemic, and serious. Rather than collecting this information about only those consumers for whom it performed tests, LabMD often collected the data of its physician-clients' entire patient roster. LabMD never deleted unneeded data, and it maintained information on 100,000 consumers for whom it never performed any tests. CCFF ¶¶ 73, 85-86, 835-841. It did not use readily-available measures to identify risks, including measures to detect and prevent unauthorized access to its networks. For example, it did not perform risk assessments or effectively deploy antivirus software and firewalls. CCFF ¶¶ 483-808. Nor did it employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, it stored backups of personal information on an employee's computer and failed to properly configure and deploy firewalls. CCFF ¶¶ 1045-1110. It did not update operating systems, including in one instance after the vendor issued an advisory identifying a security risk presented by use of a default password. CCFF ¶¶ 996-1043. It failed to develop, implement, or maintain a written information security

program. CCFF ¶¶ 397-480. It did not establish and implement password policies, such as requiring strong passwords or prohibiting shared passwords. CCFF ¶¶ 903-993. It did not prevent employees from accessing personal information not needed to perform their jobs, such as by implementing role-based access controls or minimizing available data. CCFF ¶¶ 811-849. And it did not adequately train its employees to safeguard personal information. CCFF ¶¶ 852-900.

In the few instances when LabMD did act regarding data security, it used inadequate and ineffective measures. For example, rather than using automated tools that regularly check each employee's computer for unauthorized software and files that left sensitive information vulnerable to exposure, LabMD performed walk-around inspections of its computers that were haphazard, reactive, and ineffective. CCFF ¶¶ 660-689. Compounding the problem, LabMD failed to impose basic controls on its employees' computers, giving employees administrative rights, which allowed them to download software without LabMD's knowledge, such as the peer-to-peer (P2P) software loaded onto a billing computer. CCFF ¶¶ 1050-1063. Employees are the weakest link in any security program, and non-administrative rights limit employees' control over their computers and prevent inadvertent downloading of software that could compromise not only their computers but also an entire network. CCFF ¶¶ 854, 1050-1053.

Because of these failures, which could have been remedied at no or low cost, LabMD failed to discover that LimeWire, a P2P file sharing application for which it had no business need, was installed and running on the computer used by LabMD's billing manager between 2005 and 2008. CCFF ¶¶ 691-696. The billing manager's entire "My Documents" directory was available for download through LimeWire. CCFF ¶ 1368. This directory contained more than 950 files, including LabMD's 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. The 1718 File was available on the P2P network for at least eleven months. CX0008-0011, CX0697 (1718 File) (dated June 6, 2007); CCFF ¶¶ 1363 (P2P installed on billing computer in or about 2005); 1364 (LabMD did not detect use of LimeWire prior to May 2008); 1395 (LabMD notified of availability of 1718 File in May 2008).

It was well known among LabMD employees that the billing manager had P2P software on her computer. CCFF ¶¶ 1382-1390. Yet, LimeWire remained on the billing manager's computer until May 2008 when the 1718 File and other documents were found and downloaded by an unauthorized third party using off-the-shelf P2P software available to any ordinary user.[2] CCFF ¶¶ 1364-1365, 1390-1394. LabMD did not notify the consumers whose information was contained in the 1718 File, depriving them of the knowledge that their most sensitive information had been exposed and the opportunity to identify and remedy the effects of that exposure. CCFF ¶ 1411.

A second security incident occurred in October 2012 when the Sacramento Police Department searched the home of individuals suspected of using another consumer's identity for utility services without authorization and discovered LabMD "Day Sheets," which are electronically-generated reports relating to consumer payments from LabMD's billing application. CCFF ¶¶ 150-153. They contain the sensitive personal information, such as names,

[2] This finding is uncontroverted, and is in fact supported by LabMD's witness, Richard Wallace, the former Tiversa employee who found the 1718 File using off-the-shelf P2P software. CCFF ¶ 1394. LabMD made various allegations below about Tiversa's conduct, related to issues that were not at the crux of Complaint Counsel's case. To avoid unnecessary controversy, Complaint Counsel's post-trial brief and proposed findings of fact did not cite to the testimony of Tiversa's CEO Robert Boback. Nor did they cite to CX0019, purportedly addressing the "spread" of the 1718 File, nor to any expert conclusions that were predicated on CX0019 or Mr. Boback's testimony.

Social Security numbers, and, in some cases, diagnosis codes of 600 consumers. The documents also include copies of personal checks made payable to LabMD. The individuals in possession of the Day Sheets later pleaded no contest to state charges of identity theft. CCFF ¶¶ 1413-1418, 1433-1434, 1455-1457.

III. SUMMARY OF ARGUMENT

Complaint Counsel appeals from the Administrative Law Judge's Initial Decision, which dismissed the Complaint, and concluded that Complaint Counsel did not prove that LabMD's practices caused or were likely to cause substantial consumer injury. Indeed, the Initial Decision failed to analyze LabMD's multiple, systemic, and serious security failures before issuing its ruling. ID at 13. This was a fatal flaw: whether LabMD's security practices caused or were likely to cause substantial consumer injury can be determined only through an analysis of the significant risks created by LabMD's security failures. The decision is wrong as a matter of law and fact.

A. A Significant Risk of Concrete Harm Satisfies the Section 5(n) Injury Standard

In the Commission's order denying LabMD's motion to dismiss the complaint in this case, it recognized that a practice "causes or is likely to cause substantial injury" under Section 5(n) of the FTC Act if it "raises a significant *risk* of concrete harm." Comm'n Order Denying Resp't's Mot. to Dismiss at 19 (Jan. 16, 2014) (emphasis original). The Commission clarified that a breach is not necessary in order to find substantial injury, holding "occurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury." *Id.* (internal citations and quotations omitted). The Commission cited to the Unfairness Statement for the

proposition that, even absent a breach, there can be a "significant risk of concrete harm" that constitutes "substantial injury." *Id*.. This finding is controlling in this case. The Initial Decision's disregard of this finding constitutes clear legal error.

The Commission's finding that a practice that causes a "significant risk of concrete harm" also causes "substantial injury" is supported by the legislative history of Section 5(n). In enacting Section 5(n), Congress clearly expressed its intent to codify the Unfairness Statement, which is the source of the "significant risk of concrete harm" standard. The Commission's finding is further supported by federal court decisions, which have found that a "significant risk of concrete harm" falls within the meaning of "substantial injury." *See, e.g.*, *FTC v. Neovi*, 604 F.3d 1150, 1157 (9th Cir. 2010); *Am. Fin. Servs. Ass'n. v. FTC*, 767 F.2d 957, 975 (D.C. Cir. 1985) *cert. denied*, 475 U.S. 1011 (1986).

The Initial Decision directly contradicts the Commission's order on LabMD's motion to dismiss to the extent it requires proof of actual identity theft. ID at 61-62, 64-65. The Commission does not need to wait for consumers to suffer harm at the hands of identity thieves before bringing an action. Rather, Congress has charged the Commission with a broad mandate to "*prevent* such acts or practices which injuriously affect the general public." Comm'n Order Denying Mot. to Dismiss at 4 (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess., 3 (1937)) (emphasis added).

The Initial Decision further errs by requiring Complaint Counsel to present expert testimony quantifying the probability that consumers will suffer injury as a result of LabMD's data security failures. *See, e.g.*, ID at 83-84. Section 5 imposes no such requirement, as demonstrated by its legislative history, federal court cases interpreting Section 5, and prior Commission decisions. Rather, Complaint Counsel must present "reasonably available

evidence" of the risk posed to consumers, S. Rep. No. 103-130, 1993 WL 322671, at *13 (1993), and then the cost/benefit prong of Section 5(n) must be applied.

As explained below, LabMD's multiple, systemic, and serious data security failures left many gaping holes in its network, creating a significant risk of unauthorized acquisition of consumers' sensitive information by identity thieves and others. Contrary to the Initial Decision's reasoning, *see, e.g.*, ID at 52, Section 5 liability under these circumstances does not depend on the happenstance of whether a company is breached and whether a victimized consumer can trace an identity-theft incident back to the breached company.

B. The Evidence Shows That LabMD's Practices Caused or Were Likely to Cause Substantial Injury

LabMD's practices caused substantial injury in several ways. First, LabMD's multiple, systemic, and serious data security failures caused a significant risk of concrete harm in the form of identity theft and medical identity theft. Expert testimony shows that wrongdoers seek and use the kind of information maintained by LabMD to commit identity theft and medical identity theft, CCFF ¶¶ 1642-1650, and consumers who experience identity theft and medical identity theft suffer financial harm, spend considerable amounts of time resolving it, and, in the case of medical identity theft, may suffer physical harm or even death from misdiagnoses, delays in receiving medical treatment, or unnecessary treatments. CCFF ¶¶ 1517-1562, 1593-1624. LabMD created a significant risk of these harms by collecting, storing, and transferring consumer data in large volumes on a daily basis including names, addresses, Social Security numbers, financial account and payment card numbers, medical insurance numbers, and medical test codes. CCFF ¶¶ 12, 71-161. Despite the sensitivity of the information it collected, LabMD's data security failures across all aspects of its network and operations were pervasive and serious. For example, LabMD allowed employees to use passwords such as "labmd," CCFF

¶¶ 909-983, failed to update out-of-date software that vendors no longer supported, CCFF ¶¶ 996-1040, and did not technologically prevent employees from downloading software. CCFF ¶¶ 1050-1063.

Second, LabMD's exposure of consumers' sensitive personal information of the 1718 File for almost a year on a P2P network increased the already-significant risk of concrete harm that LabMD's inadequate data security practices created. The Initial Decision downplayed this magnified risk by stating that no identity theft victims came forward, showing that identity thieves did not access the file. ID at 64. However, LabMD never provided consumers with notice of this incident, CCFF ¶ 1411, so it would have been impossible for identity theft victims to tie the crime of identity theft to LabMD's security failures. The Initial Decision further concluded that it was unlikely that unauthorized parties would have accessed the file because they could only have found it by searching the filename "insuranceaging." ID at 24, ¶ 77. In reaching this conclusion, the Initial Decision ignored uncontroverted expert testimony that unauthorized parties often accessed files by conducting searches of a users' entire sharing folder; types of folders commonly shared by mistake, such as "Windows" or "My Documents;" or document type, such as .pdf. CCFF ¶¶ 1273-1296. Indeed, the Initial Decision ignored the fact that Richard Wallace – an unauthorized third party who found the 1718 File – used a standard P2P client as part of a general search for sensitive information. CCFF ¶ 1394; Wallace, Tr. 1372. This demonstrates that any of the millions of other P2P users, conducting millions of searches a day over an eleven month period – especially those seeking to download and exploit sensitive information – had the opportunity and ability to do the same, creating a heightened significant risk of harm.

Third, in addition to the significant risks of concrete harm imposed upon consumers by LabMD's unlawful data security practices and the exposure of the 1718 File on a P2P network for nearly a year, the unauthorized disclosure of the 1718 File to unauthorized parties also caused harm for consumers, because they experienced the loss of privacy of their sensitive personal and health information. Federal and state law recognize individuals' right to privacy in personal information, particularly medical information. *See, e.g.*, HIPAA, P.L. 104–191 § 264, 110 Stat. 1936 (Aug. 21, 1996); Ga. Code Ann. §§ 31-33-2(d), 31-33-6 (empowering medical providers to keep medical records confidential); Ga. Code Ann. §§ 31-22-9.1(a)(2)(D), 24-12-21(b)(1) (limiting the release of "AIDS confidential information," including that a person a has submitted to an HIV test). These laws demonstrate the broad recognition of the inherent harm in the exposure of medical information. The exposure need not result in further injury—the mere disclosure is the harm. Indeed, Georgia courts have allowed payment of monetary damages to victims whose private data – of a type similar to the data at issue in this case – was exposed. *See, e.g., Bazemore v. Savannah Hospital*, 155 S.E. 194 (Ga. 1930); *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 496 (Ga. Ct. App. 1994); *Zieve v. Hairston*, 598 S.E.2d 25, 31 (Ga. Ct. App. 2004). Consumers included in the 1718 File, whose sensitive personal information exposed includes CPT codes indicating tests for HIV, hepatitis, herpes, prostate cancer, and testosterone levels, CCFF ¶¶ 1684-1697, suffered substantial injury from this unauthorized disclosure.

IV. PROCEDURAL HISTORY

On August 29, 2013, the Commission issued an administrative complaint charging Respondent with violating Section 5(a) of the FTC Act by failing to employ reasonable and appropriate measures to prevent unauthorized access to personal information, which caused or

likely caused substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. On September 17, 2013, Respondent filed an answer denying that it violated the FTC Act. After eight days of witness testimony, including a delay for one of Respondent's witnesses to obtain immunity from prosecution for his testimony, the evidentiary record closed on July 20, 2015. On November 13, 2015, Administrative Law Judge D. Michael Chappell issued his Initial Decision and Order. Complaint Counsel filed a Notice of Appeal on November 24, 2015.

V. QUESTION PRESENTED

Whether the evidence as a whole shows that LabMD's multiple, systemic, and serious security failures caused or were likely to cause substantial injury to consumers that was not reasonably avoidable by consumers themselves and not offset by countervailing benefits to consumers or competition, in violation of Section 5(a) of the FTC Act.

VI. ARGUMENT

Section 5(n) defines an unfair practice as one that (1) "causes or is likely to cause substantial injury to consumers" which is (2) "not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). The Initial Decision reached only the first prong of Section 5(n), concluding that Complaint Counsel failed to prove that LabMD's data security failures "caused, or is likely to cause, substantial consumer injury." ID at 49; 90-91 ¶¶ 18, 23-24, 27, 29, 31. In so holding, the Initial Decision failed to recognize that "significant risk of concrete harm" itself causes substantial consumer injury within the meaning of Section 5(n). The Initial Decision also failed to evaluate how LabMD's multiple, systemic, and serious data security failures created a significant risk of concrete harm in the form of identity theft and medical

identity theft, incorrectly analyzed the significance of the risk to consumers of the 1718 File's exposure on a P2P network for nearly a year, and failed to recognize the harm caused to consumers by disclosure of their sensitive medical information

A. The Initial Decision is Incorrect as a Matter of Law

The Initial Decision ignored the Commission's key finding from its order denying LabMD's motion to dismiss: that a practice causes or is likely to cause substantial injury under Section 5(n) of the FTC Act if it "raises a significant risk of concrete harm." Proof of actual identity theft is not required. Nor does Complaint Counsel need to prove the probability of injury with mathematical precision. Finally, the test for establishing injury under Section 5(n) is not comparable to the test for establishing standing for a private party under Article III.

1. An Act or Practice That Raises a Significant Risk of Concrete Harm Causes Substantial Injury

In the Commission's order denying LabMD's motion to dismiss the complaint in this case, it recognized that a practice "causes or is likely to cause substantial injury" under Section 5(n) of the FTC Act if it "raises a significant *risk* of concrete harm." Comm'n Order Denying Mot. to Dismiss at 19 (emphasis original) (quoting Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("Unfairness Statement"), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1984 LEXIS 2, at *307 n.12 (1984)). Importantly, even though the 1718 File was exposed on the P2P network, the Commission clarified that such a breach is not necessary in order to find substantial injury, holding "occurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury." *Id.* (internal citations and quotations omitted). The Commission cited to the Unfairness

Statement for the proposition that, even absent a breach, there can be a "significant risk of concrete harm" that constitutes "substantial injury." *Id.* This finding is controlling in this case. The Initial Decision's disregard of this finding constitutes clear legal error.

The Commission's order denying LabMD's motion to dismiss cites to the Unfairness Statement, which stated that "significant risk of concrete harm" is itself "substantial injury." It states that an *injury* is "sufficiently substantial . . . if it does a small harm to a large number of people, or if it *raises a significant risk of concrete harm*." Unfairness Statement, 1984 LEXIS 2 at *307 n.12. (emphasis added). The Unfairness Statement further contemplates that "[u]nwarranted health and safety *risks*" can support a finding of unfairness. *Id*. at *248 (emphasis added); *see also id.* at *248 n.45. Indeed, the Unfairness Statement does not equate "significant risk of concrete harm" as being "likely" to cause injury; it states that "significant risk of harm" is substantial injury in itself.

Federal courts have similarly found that a "significant risk of concrete harm" falls within the meaning of "substantial injury." *See, e.g., FTC v. Neovi*, 604 F.3d 1150, 1157 (9th Cir. 2010) ("An act or practice can *cause substantial injury* by doing a small harm to a large number of people, or if it raises a significant risk of concrete harm.") (emphasis added; internal quotations omitted); *Am. Fin. Servs. Ass'n.*, 767 F.2d at 975 (finding that the potential use of household good security interests and wage assignments by creditors creates "a significant risk of substantial economic and monetary harm to the consumer as well as potential deprivations of their legal rights," thus "establishing substantial consumer injury").[3]

[3] While *American Financial Services Association* was decided before the enactment of Section 5(n), it applied the Unfairness Statement's later-codified three-part test for injury. 767 F.2d at 971.

The Initial Decision incorrectly concludes that the legislative history of Section 5(n) demonstrates that Congress "considered but rejected" the Commission's view that injury includes a "significant risk of concrete harm." ID at 54-55. In support, the Initial Decision cites a lone, out-of-context statement from the Senate Report discussing proposed Section 5(n), which states, in part, "Consumer injury may be 'substantial' under this section if a relatively small harm is inflicted on a large number of consumers or if a greater harm is inflicted on a relatively small number of consumers." *Id.* at 54 (quoting S. Rep. 103-130, 1993 WL 322671, at *13). Because this sentence does not contain the Commission's "significant risk" language, the Initial Decision concludes that Congress intended to exclude this interpretation from the statute. ID at 54.

This is not a reasonable analysis of Section 5(n)'s legislative history. First, in the paragraph immediately preceding the sentence quoted in the Initial Decision, the Senate Report states that Section 5(n) is intended to codify the Unfairness Statement to allow the FTC to continue the development of "existing law." Specifically, it states:

> This section is intended to codify, as a statutory limitation on unfair acts or practices, the principles of the FTC's December 17, 1980, policy statement on unfairness, reaffirmed by a letter from the FTC dated March 5, 1982. *Since the FTC's policy statement itself is based on the FTC's decided cases and rules, this section codifies existing law.* The incorporation of these criteria should enable the FTC to proceed in its development of the law of unfairness with a firm grounding in the precedent decided under this authority, and consistent with the approach of the FTC and the courts in the past.

S. Rep. 103-130, 1993 WL 322671, at *12-13 (emphasis added). Second, the Senate Report expressly recognizes that substantial injury can include "unwarranted health and safety *risks*." *Id.* at *13 (emphasis added). Third, the House Conference Report affirms the Senate's intent to codify the Unfairness Statement. It states that Section 5(n) "is derived from the 1980 policy statement of the Commission regarding unfairness, the Commission's 1982 letter on the same

subject, and from subsequent interpretations of and applications to specific unfairness proceedings by the Commission." *See* H.R. Conf. Rep. 103-617, 1994 WL 385368, at *11-12 (July 12, 1994). Indeed, courts have subsequently recognized this Congressional intent. *See, e.g.*, *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 937 n.5 (N.D. Ill. 2008) ("The legislative history demonstrates that Congress's intent was to codify the FTC's Unfairness Policy Statement of 1980 . . . .").

Accordingly, to the extent the Initial Decision concludes that Congress enacted Section 5(n) to limit the FTC's unfairness authority more narrowly than the construction of the Unfairness Statement, such a view is unsupported. Considered in context, there is no reasonable basis to conclude that Congress intended to leave consumers without protection by excluding "significant risks of concrete harm" from the meaning of "substantial injury" under the statute, or otherwise limiting the Unfairness Statement.

Contrary to the Initial Decision's reasoning, there is nothing inconsistent with the statute's codification of the term "substantial injury" to include "significant risk of concrete harm" and its provision of additional, alternative grounds for the Commission to take action against practices that are likely to cause such injury in the future. By setting out the two alternative justifications for Commission action, the statute gives the agency authority to act either where a practice currently causes a significant risk of concrete harm, or where a practice is likely to do so in the future. The statute distinguishes the temporal nature of the substantial injury that each alternative is intended to address by use of verb tense – "causes . . . substantial

injury" for practices that currently cause a significant risk of concrete harm and "is likely to cause substantial injury" for those that are likely to cause such injury in the future.[4]

As an example of the distinction, a debt collection company that posts a list of debtors' names and Social Security numbers on the Internet causes substantial injury because its posting of this sensitive information causes a significant risk of concrete harm in the form of identity theft. A similarly-situated company that makes arrangements to post names and Social Security numbers on the Internet in the future is *likely* to cause substantial injury, even before the

[4] As discussed in detail in Section VI.A.2, *infra*, the plain language of the statute makes clear that the appropriate time frame to analyze whether a practices causes a significant risk of concrete harm or is likely to cause such a risk in the future is the time that the practice at issue occurs, not the time that the complaint is filed or litigated. "[T]he *act or practice* causes or is likely to cause substantial injury …." 15 U.S.C. § 45(n) (emphasis added); *see also* Comm'n Order Denying Mot. to Dismiss at 19 (breach not necessary to "substantiate that the firm's data security activities caused or likely caused consumer injury").

information is posted, because its actions are likely to create a significant risk of concrete harm. In both instances, Section 5 would authorize the Commission to take action to prevent harm.[5]

The Commission's order denying LabMD's motion to dismiss clearly established that unreasonable data security practices cause substantial injury, even where there has been no breach. Comm'n Order Denying Mot. to Dismiss at 19. The Initial Decision directly contradicts the Commission's order to the extent it requires proof that (1) LabMD's files were accessed by third parties and (2) such unauthorized third parties were acting with malicious intent. ID at 61-62, 64-65. The Commission does not need to wait for consumers to suffer harm at the hands of identity thieves before bringing an action. Rather, Congress has charged the Commission with a broad mandate to "*prevent* such acts or practices which injuriously affect the general public." Comm'n Order Denying Mot. to Dismiss at 4 (quoting H.R. Rep. No. 1613, 75th Cong., 1st

---

[5] An alternative explanation for Congress's addition of the word "likely" is that, consistent with its clear intent to codify the Unfairness Statement, S. Rep. 103-130, 1993 WL 233671, at *12-13, Congress simply used a shorter formulation to encapsulate the lengthy test contained in the Unfairness Statement. Rather than saying that a practice is unfair if it "causes substantial injury" if "it raises a significant risk of concrete harm," raising(which would have made the three-part unfairness test unwieldy), Congress may have simply decided to use fewer words. An act or practice is unfair if it "causes or is likely to cause substantial injury." The interpretation that the term "likely" is shorthand for "significant risk of concrete harm" is consistent with common understandings of the term "likely." Although the Initial Decision cites to an isolated definition from one dictionary to conclude that "likely" means "probable," ID at 54; 90 ¶ 22, the Oxford English Dictionary also defines "likely" as "[h]aving an appearance of truth or fact," *available at* http://www.oed.com/view/Entry/108315? rskey=fSsgCg&result=1& isAdvanced=false#eid, while Dictionary.com offers a definition as "reasonably to be believed or expected." *Available at* http://dictionary.reference.com/browse/likely. Merriam-Webster – the dictionary cited by the Initial Decision – also defines "likely" as "seeming to be true." *Available at* http://www.merriam-webster.com/ dictionary/likely.

The Initial Decision also improperly relies on the Commission's standard for deception, which requires proof that a practice is "likely to mislead" consumers. ID at 90 ¶ 21. The Commission's deception standard is not relevant to Section 5(n), which solely addresses unfairness. *See Yates v. U.S.*, 135 S.Ct. 1074, 1082 (2015) (noting that "identical language may convey varying content when used in different statutes, sometimes even in different provisions of the same statute."). In any event, regardless of other definitions or uses of the term "likely," the meaning of terms in a statute "is determined [not only] by reference to the language itself, [but also by] the specific context in which that language is used, and the broader context of the statute as a whole." *Yates*, 135 S.Ct. at 1081-82 (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997) (alterations in original)) Given the context here, the Commission has found and should affirm that an act or practice meets the Section 5(n) standard if it raises a significant risk of concrete harm, irrespective of whether the "significant risk" concept is encompassed in the term "substantial injury" or "likely."

Sess., 3 (1937)) (emphasis added); *see also FTC v. Gratz*, 253 U.S. 421, 435 (1920) (Brandeis, J., dissenting) ("[The Commission] was to be ever vigilant. If it discovered that any business concern had used any practice which would be likely to result in public injury . . . the Commission was directed to intervene . . . . Its action was to be prophylactic. Its purpose in respect to restraints of trade was prevention of diseased business conditions, not cure.").[6] The legal analysis should end here. Nonetheless, the Initial Decision raises several additional points, addressed below.

2. Section 5(n) Does Not Require Proof of Known Identity Theft

The Initial Decision errs to the extent it requires Complaint Counsel to enter evidence of consumers who have suffered identity theft. ID at 52-53. As discussed above, it ignores the Unfairness Statement and the Commission's decision in this case, which specifically holds that "substantial injury" includes a "significant risk of concrete harm." This requirement also ignores the plain wording of Section 5(n), which states that an act or practice that is "likely to cause substantial injury" satisfies the first prong of the unfairness analysis. 15 U.S.C. § 45(n).

Instead of addressing the plain language of the statute, or its legislative history, the Unfairness Statement, or the Commission's prior ruling, the Initial Decision points to other unfairness decisions, noting that there does not appear to be "any case where unfair conduct liability has been imposed without proof of actual harm." ID at 53. Notably, however, the Initial Decision fails to cite the Commission's previous decision in *this* case, which, as noted,

[6] Although *Gratz* was decided in the antitrust context of unfair methods of competition, its rationale is no less applicable to unfair acts or practices affecting consumers. *See, e.g.*, *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972) (observing that the Wheeler-Lea amendment of 1938 "makes the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor." (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess., 3 (1937) (internal quotations omitted)).

determined that Section 5(n) permits the Commission to challenge multiple and systemic data security failures even where no breach has occurred.[7] *Supra* § VI.A.1.

To the extent the Initial Decision finds Complaint Counsel's harm theory unpersuasive because of the absence of any evidence of consumer harm, "even after the passage of many years," ID at 52, this suggestion is undermined by the nature of identity theft. Where, as here, consumers are not notified that their information has been disclosed, they would have no way of tracing identity theft to a particular business's unreasonable data security practices.

In any event, an *ex post* analysis of injury is not relevant. The question is whether an act or practice causes or is likely to cause substantial injury *at the time of the unfair conduct*. *See, e.g., Int'l Harvester Co.*, , 104 F.T.C. 949, 1984 FTC LEXIS 2, at *252 n.52 (1984) (noting that review of risk presented by unfair conduct should not be based on "an *ex post* review of events rather than being, as it should be, a before-the-fact assessment of the risks to which consumers may be subjected"). Analyzing unfair practices as of the time they occurred provides appropriate incentives to a firm to forego harmful conduct, rather than merely to remedy it after the fact. Otherwise, an entity could avoid Section 5 liability by hastily correcting its unfair conduct in response to an FTC investigation. Indeed, whether a practice is unfair does not depend on the happenstance of whether a company is breached and whether a victimized consumer can trace an identity theft incident back to the breached company. Fundamentally, in this case, the time of the conduct to be examined is the time of LabMD's failure to protect

[7] The Initial Decision also ignores cases where the Commission has obtained preliminary relief based on likely harm under Section 5(n). *See, e.g., FTC v. CyberSpy Software, LLC*, No. 08-CV-1872 (M.D. Fla.) (Preliminary Injunction entered Nov. 25, 2008), Complaint at 12, ¶ 41 ("[T]he sale and operation of RemoteSpy is likely to cause substantial harm to consumers …."), *available at* https://www ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf.

sensitive consumer information, not the time of any *exposure* of sensitive personal information. *See* CCPTB at 2-3.

3. Section 5(n) Does Not Require That Substantial Injury Be Established With Mathematical Precision

The Initial Decision incorrectly requires Complaint Counsel to present expert testimony quantifying the probability that consumers will suffer injury as a result of LabMD's data security failures. *See, e.g.*, ID at 83-84. Section 5 imposes no such requirement, as demonstrated by its legislative history, federal court cases interpreting Section 5, and prior Commission decisions.

In codifying the Commission's Unfairness Statement, Congress was explicit that mathematical quantification is not required in order to conduct a cost/benefit analysis under Section 5:

> In determining whether a substantial consumer injury is outweighed by the countervailing benefits of a practice, the Committee does not intend that the FTC quantify the detrimental and beneficial effects of the practice in every case. In many instances, such a numerical benefit-cost analysis would be unnecessary; in other cases, it may be impossible. This section would require, however, that the FTC carefully evaluate the benefits and costs of each exercise of its unfairness authority, gathering and considering reasonably available evidence.

S. Rep. No. 103-130, 1993 WL 322671, at *13 (1993). This is consistent with *American Financial Services Association*, in which the D.C. Circuit found "no basis for imposing" a requirement for "quantitative economic analysis," deferring to the Commission's policy letter, in which it had stated that "a highly quantitative benefit/cost analysis may not be appropriate" in every case. *Am. Fin. Servs. Ass'n*, 767 F.2d at 986 (quoting Letter from FTC Chairman J.C. Miller, III to Sens. Packwood and Kasten (Mar. 5, 1982), *reprinted in* H.R. Rep. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32-33 (1983)).

The same rationale that applies for not requiring precise quantification of a cost/benefit analysis applies to the injury prong of unfairness. Indeed, numerous courts have confirmed that injuries caused by unfair practices need not be monetarily quantifiable. *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1364-65 (11th Cir. 1988) (affirming Commission grant of summary judgment where injury included in part "intangible loss" relating to certainty of contract terms). For example, 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) (obtaining and selling consumers' confidential phone call records is an unfair practice under Section 5); *see also Am. Fin. Servs. Ass'n*, 767 F.2d at 974-75 & n.20 (affirming Commission's finding of harm where consumers suffered not only monetary loss and "the significant risk of substantial economic and monetary harm," but also psychological impact from loss of household goods, loss of sentimental value of seized goods, vulnerability to predatory financial practices, effect on physical health, and disruption of family relationships). Further, the Commission has stated that unquantifiable health and safety risks can also be unfair. *See Philip Morris, Inc.*, Docket No. 8838, 82 F.T.C. 16, 17 (Jan. 9, 1973) (alleging unfairness where the distribution of razor blades in newspapers "constitutes a hazard to . . . health and safety") (cited in Unfairness Statement, 1984 FTC LEXIS 2, at *308 n.15).

The Initial Decision misapprehends *International Harvester* as requiring injury to be mathematically quantified. ID at 81-82. While the Commission did state that no useable rule of liability could be derived "[w]hen divorced from *any* measure of the probability of occurrence," this was preceded by the Commission's determination to "endeavor to assess this risk from the most probative indirect evidence that is available." *Int'l Harvester*, 1984 FTC LEXIS 2, at *253

n.52 (emphasis added). *International Harvester* involved a calculable 0.001% risk of significant harm, derived from exhaustive data of past fuel geysering incidents, and the Commission determined that this "empirical incidence of harm . . . is the best available measure of risk." *Id.* at *89 & n.52. The Commission recognized, however, that such extensive data is not always available. *Id.*

In a data security case, often there can be no precise calculable risk of injury. It may be impossible to predict with mathematical precision how many consumers' information will be exposed to unauthorized access, how wide the exposure will be, the precise data that will be exposed, the length of the exposure, the dollar value of the harms, and other relevant factors. This does not mean that Section 5 cannot be applied where data security failures have not yet resulted in harm that can be expressed as a precise numerical percentage. Rather, Complaint Counsel must present "reasonably available evidence" of the risk posed to consumers, S. Rep. No. 103-130, 1993 WL 322671, at *13 (1993), and then the cost/benefit Section 5(n) test must be applied.[8]

4. Section 5(n)'s Substantial Injury Standard Is Broader Than Article III's Standing Standard

The Initial Decision's reliance on cases concerning the standard of injury for Article III standing is misplaced. *See, e.g.*, ID at 85 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011)). While the *Reilly* case found that individual plaintiffs lacked standing because some

[8] Of course, this does not mean that the "significant risk of harm" standard is boundless. Trivial, speculative, or certain subjective harms, such as those that offend the tastes or social beliefs of particular consumers do not meet the first prong of Section 5(n). Unfairness Statement, 1984 FTC Lexis 2, at *307. Moreover, the third prong of the Section 5(n)'s unfairness test also addresses the Initial Decision's concerns about speculative harm. ID at 53, 85. The harm must first be substantial, and then must not be outweighed by benefits to consumers or competition. In any event, the significant monetary and non-monetary risks associated with identity theft and medical identity theft have been well documented, and an unreasonable failure to protect the information used to commit such crimes unquestionably causes or is likely to cause substantial injury.

future act by a third party would be required to cause injury, the FTC Act analysis is fundamentally different than the analysis required to find Article III standing.

First, the 5(n) standard is facially broader than the standard required for Article III standing; nothing in Section 5(n) requires injury-in-fact. Rather, an act or practice that causes or is likely to cause substantial injury is sufficient. And as noted above, as the entity charged with interpreting Section 5(n), the Commission has held that a significant risk of concrete injury constitutes substantial injury. *Supra* § VI.A.1.

Second, Congress has conferred standing on the Commission to enforce Section 5. *See, e.g.*, *FTC v. CyberSpy Software, LLC*, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009); *SEC v. Rogers*, 283 Fed. App'x 242, 243 (5th Cir. 2008) ("Congress may confer standing on federal agencies to bring enforcement actions under its statutes."). Whether a private plaintiff has standing to challenge a data security practice under Article III is not relevant to injury within the meaning of Section 5(n). The FTC Act expressly does not require the Commission to wait for consumer injury to occur before bringing an action. *See, e.g.*, Comm'n Order Denying Mot. to Dismiss at 19; *Am. Fin. Servs. Ass'n*, 767 F.2d at 972; 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").

B. The Initial Decision is Incorrect as a Matter of Fact

LabMD's practices in this case caused substantial injury in several ways. First, LabMD's multiple, systemic, and serious data security failures caused a significant risk of concrete harm in

the form of identity theft and medical identity theft. Second, LabMD's exposure of consumers' sensitive personal information in the 1718 File for almost a year on a P2P network increased the already-significant risk of concrete harm that LabMD's inadequate data security practice created. Third, in addition to the significant risk of concrete harm caused to consumers by its exposure on the P2P network, disclosure of the 1718 File to an unauthorized third party also caused harm for consumers, because they experienced the loss of privacy of their sensitive personal and health information.

1. LabMD's Data Security Practices Created a Significant Risk of Concrete Harm

The overwhelming evidence presented in this case demonstrates that LabMD's multiple, systemic, and serious data security failures created a significant risk of concrete harm to the consumers whose data the company held. LabMD collected, stored, and transferred extremely sensitive consumer data in large volumes on a daily basis, including names, addresses, Social Security numbers, financial account and payment card numbers, medical insurance numbers, and medical test codes. Despite the sensitivity of the information it collected, LabMD's data security failures across all aspects of its network and operations were pervasive and serious. *Cf.* CCFF ¶ 392. This finding alone is sufficient to hold LabMD liable under Section 5. In addition, by exposing the 1718 File on a P2P network, LabMD heightened the already significant risk its unlawful data security practices created. Expert testimony shows that wrongdoers seek and use the kind of information maintained by LabMD to commit identity theft and medical identity theft, which can harm consumers financially or negatively affect their medical care, health, and other aspects of their lives.

a. LabMD's Data Security Failures Were Multiple, Systemic, and Serious, Placing Consumers at a Significant Risk of Concrete Harm

LabMD collected and stored large amounts of sensitive personal information that is highly valued by identity thieves for its usefulness in perpetrating frauds, including Social Security numbers, bank routing and account numbers, credit and debit card numbers, health insurance policy numbers, and medical diagnosis and test codes.[9] CCFF ¶¶ 12, 393, 1642-1650; *see also*, *infra* § VI.B.2.c. LabMD received this sensitive personal information over public networks and stored it on servers and computers connected to the Internet, CCFF ¶¶ 84-115, 163-170, which can create a "fertile environment for hackers and others to exploit computer system vulnerabilities, covertly obtain access to consumers' [personal information], and potentially misuse it in ways that can inflict serious harms on consumers." Comm'n Order Denying Mot. to Dismiss at 1; *see also* CCFF ¶¶ 81-82, 89-90, 92-94, 1472-1721. Its data

[9] The Initial Decision failed to analyze LabMD's security practices before ruling that the practices were unlikely to cause substantial consumer injury. ID at 13. This was a fatal flaw: whether LabMD's security practices cause a significant risk of concrete harm to consumers or likely caused substantial injury can only be determined by an analysis of its security failures.

The Initial Decision errs in attempting to separate reasonableness of data security practices from the risk of injury when it posits that: "a 'risk' of harm is inherent in the notion of 'unreasonable' conduct. To allow unfair conduct liability to be based on a mere 'risk' of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone." ID at 81 (probability of injury is discussed *infra* in § VI.A.3). This is erroneous. A showing of unreasonable security *itself* satisfies Section 5(n), because unreasonable security practices cause or are likely to cause substantial consumer injury that is not outweighed by the benefits to consumers or competition and is not reasonably avoidable by consumers.

security failures subjected consumers to a significant risk of concrete harm, by increasing the risk for exposure and compromise.[10]

To illustrate the significant risk of harm posed by unlawful security and the consequent vulnerabilities to unauthorized access it introduces, Complaint Counsel's expert Mr. Van Dyke presented the results of Javelin's Identity Fraud surveys of consumers from 2010 through 2013. The surveys showed that data breach victims experienced identity fraud at rates seven to eleven times that of consumers who had not been notified they were involved in a data breach, constituting absolute rates of 11.8% to 30.5%, with the risk increasing year over year. CX0741 (Van Dyke Report) at 7 & 8 Fig. 1.

And yet, LabMD utterly failed to implement the security needed to mitigate the risk of breaches and to adequately protect the large amounts of highly sensitive personal information it collected. *See Comm'n Statement Marking 50th Data Security Settlement* (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf. By

---

[10] The ALJ wrongfully excluded Complaint Counsel's computer security expert's opinion that LabMD's security vulnerabilities "increased the risk for exposure and compromise" Hill, Tr. 318, 320-322. Because that exact phrasing did not appear in her report, the ALJ incorrectly ruled that it was a new opinion and should be excluded. *Id.* at 320-322. Expert reports, however, are not required to be transcripts of the expert's later trial testimony, and testimony should be allowed when it is consistent with the opinions expressed in that expert's report. *See, e.g., Metavante Corp. v. Emigrant Sav. Bank*, 619 F.3d 748, 762 (7th Cir. 2010) (stating that purpose of expert's report "is not to replicate every word that the expert might say on the stand," but "to convey the substance of the expert's opinion … so that the opponent will be ready to rebut, to cross-examine, and to offer a competing expert if necessary") (citations omitted); *Rockhill-Anderson v. Deere & Co*., 994 F. Supp. 2d 1224, 1239 (M.D. Ala. 2014) (refusing to strike expert affidavit because "consistent" with previously disclosed reports and deposition testimony); *Gay v. Stonebridge Life Ins. Co.* 711 F. Supp. 2d 165, 167 (D. Mass 2010) ("Although an expert report must contain a 'complete statement of all opinions the witness will express,' that statement need not include the precise language that the expert will employ at trial." (citations omitted)).

Here, the excluded opinion meets that standard: Dr. Hill's *entire* report discusses in detail why LabMD's specific practices created security vulnerabilities that could be remedied with low cost measures that "reduce[] the likelihood that an attack will succeed," in support of her overall conclusion that LabMD "failed to provide reasonable and appropriate security for Personal Information." CX0740 (Hill Report) at ¶¶ 17, 27, 49, 51-107. While Dr. Hill's opinions on LabMD's specific practices are in the record and sufficient for finding liability, the Commission should also admit, consider, and rely upon her testimony on the overall increased risk of unauthorized disclosure that LabMD's security practices created.

failing to implement simple, well-known, and low cost security measures, LabMD significantly increased the risk of unauthorized exposure. *See* CCFF ¶¶ 382-1185.

LabMD had numerous, serious, and systemic flaws in its network security practices. It increased the risk of unauthorized disclosure in the following ways:

- LabMD was blind to vulnerabilities that intruders (or insiders) could use to obtain unauthorized access to personal information on the network. Prior to 2010, LabMD did not use any penetration tests or other automated tools, such as intrusion detection systems (IDS) or file integrity monitoring (FIM), that would have identified commonly known or reasonably foreseeable security risks and vulnerabilities on its network. Indeed, when LabMD finally conducted penetration testing in 2010 at the cost of $450 for nine servers, the testing revealed 32 vulnerabilities on a server handling vast amounts of personal information, including one easily-exploited – yet easily-corrected, once discovered – vulnerability that could have allowed intruders to control the server and obtain consumers' personal information. LabMD could have used automated tools to test for commonly known security risks at little or no cost. CCFF ¶¶ 483-496, 700-808, 1134, 1140, 1145-1146.

- LabMD did not technologically limit the computer user rights for its employees. LabMD could not control the ability of employees to indiscriminately download and install programs like LimeWire from the Internet. LabMD could have addressed this risk at no additional cost by using the Windows operating system to assign employees non-administrative rights. CCFF ¶¶ 458-480, 1050-1063.

- LabMD did not use readily available measures to prevent or detect unauthorized access to personal information. For example, it did not use automated tools to monitor LabMD computers with access to personal information for any improper downloads. Such unauthorized downloading of software presented an opportunity for an intrusion to happen. Hill, Tr. 97-98, 225-26, 284. It also failed to properly configure firewalls, such as implementing IP address filtering, which would have prevented communication with the network by an untrusted source. Further, it stored backups on workstation computers, which puts the information stored on the computer at risk of exposure in the course of the employee's workflow. LabMD could have remedied these issues at the cost of employee time by using the Windows operating system to assign employees non-administrative rights, and by properly configuring its existing firewall software. CCFF ¶¶ 458-480, 1050-1072, 1094-1095.

- LabMD did not maintain and update operating systems and other devices to protect against known vulnerabilities, which is necessary because hackers often exploit software bugs to gain unauthorized access to networks. For example, LabMD failed to update its Veritas backup application to close a vulnerability an

attacker could use to take partial control of LabMD servers and steal consumers' personal information. Hill, Tr. 191. Updating software to install patches and vulnerability updates can typically be done at a low cost. For software that is so out-of-date it is no longer being supported by the vendor, it may be necessary to replace the program with a newer, supported version. CCFF ¶¶ 997-998, 1017-1043, 1642-1650, 1171-1173.

- When it did take security measures, LabMD implemented limited, reactive, and *ad hoc* security measures that left open security holes, as evidenced by the above failures. Prior to 2010, LabMD did not have any written information security plan, which would have provided its IT employees with a roadmap for identifying security risks and choosing which security measures were necessary to protect against those risks.[11] Any time there is Internet access, there is a possibility of intrusion, and policies and enforcement mechanisms must be in place to limit what an employee can do. Hill, Tr. 287. LabMD could have created a written comprehensive information security plan at little to no cost by using free online resources available from national experts. CCFF ¶¶ 397-446, 489-512, 767, 803,1121-1124.

LabMD also failed to protect consumer personal information when it was transferred over public networks:

- LabMD significantly increased the risk that hackers could compromise its entire network when it set up its file transfer program (FTP), which allowed physician offices to upload sensitive consumer personal information to LabMD's servers, to permit anonymous log-ins without any password or unique credentials. This could have been remedied by simply disallowing anonymous log-ins. CCFF ¶¶ 781-788.

- LabMD did not provide its employees with the tools or training to encrypt emails containing sensitive personal information. For example, from 2004 to at least 2006, an IT employee transferred personal information from LabMD's network to the private AOL email account of LabMD's CEO without encrypting the information. CCFF ¶¶ 477-480.

[11] After 2010, LabMD points to its Employee Handbook, Compliance Program, and employee training as providing sufficient written security policies. CCFF ¶ 423. However, these materials say almost nothing about security. CCFF ¶¶ 425-431, 452-480, 919-923. LabMD's CEO and IT personnel could not identify any specific measures referred to in the Handbook adopted to comply with HIPAA's privacy provisions. CCFF ¶¶ 437-438 (author of LabMD's Compliance Program admitted it did not include any security policies), CCFF ¶¶ 852, 854, 857-863, 1159-1162 (lack of meaning security training for employees). Moreover, LabMD did not enforce the few security policies that were included in these materials. CCFF ¶¶ 458-480.

Further, LabMD did not adopt, implement or enforce an effective password policy, which increased the risk of unauthorized disclosure because it leaves the network vulnerable to password-guessing attacks, CCFF ¶¶ 904, 909:

- LabMD did not require its employees to use strong password practices, such as minimum password length, using numbers or special characters, not using dictionary words, and requiring unique credentials for each program. Instead, LabMD allowed its employees to use the same easy-to-guess passwords for years, such as one employee who used the password 'labmd' from 2006 to 2013. As LabMD's own IT employee stated, LabMD's passwords in 2009 were "less than adequate" and "not as complex as they should have been." CCFF ¶ 911, 913. LabMD could have implemented a password policy that required passwords to be unique, strong, and changed periodically through a Windows centralized password management scheme that was included in its operating system. CCFF ¶¶ 906-941, 990-993.

- LabMD did not implement strong password policies for its servers. Instead, from October 2006 through April 2009 every server login username was "admin," and every password was "LABMD." LabMD also set up its servers to use a universal default administrator user, instead of using different credentials for each IT employee. CCFF ¶ 968-971.

- LabMD also did not have any password policies for its physician-clients when they uploaded sensitive personal information from their offices to LabMD's servers with FTP software. Instead, LabMD allowed physician offices to use, and share in some cases, simple usernames and passwords. CCFF ¶¶ 974-983.

LabMD also did not limit the scope of personal information vulnerable to attack, increasing the risk of unauthorized disclosure and needlessly increasing the scope of potential harm from a malicious insider or from a network compromise, CCFF ¶¶ 71-79, 811-814, 832-849:

- LabMD did not restrict employee access to only the personal information that was necessary for the employee to perform his or her job. LabMD easily could have restricted user access to unnecessary personal information by enabling controls already embedded in its operating system. CCFF ¶¶ 811-821, 1149-1151.

- LabMD collected more personal information than was necessary to run its business, including personal information from patients for whom it never performed any laboratory services, and retained personal information for longer than was necessary, sometimes indefinitely. LabMD could have reduced the

unnecessary personal information it collected and stored by simply deleting data it no longer needed on a regular basis. CCFF ¶¶ 71-87, 126, 138, 146-160, 832-849.

Finally, LabMD did not provide security training to its employees:

- LabMD did not train its non-IT employees on data security, data security policies, security tools, or the consequences of reconfiguring security settings in applications. This increased the risk of unauthorized disclosure because users are the weakest link in any information security program. Many LabMD employees had the ability to change their security settings and had access to voluminous, highly sensitive personal information. LabMD could have provided data security training to its employees at little to no cost. CCFF ¶¶ 852-869, 879-900, 1056-1060, 1157-1162.

- LabMD did not provide IT employees with any type of formal or informal information security training. This increased the risk of unauthorized disclosure because IT practitioners are the front line defense against intrusion and need regular training to stay current with evolving security threats, vulnerabilities and safeguards. LabMD could have trained its IT employees through free or low-cost security courses offered by several nationally recognized organizations. CCFF ¶¶ 417, 852-863, 1116, 1157-1162.

Although LabMD used antivirus software, simple firewall software, and manual inspections, these limited measures did not and could not effectively assess or mitigate the very real risks to the LabMD network the way penetration testing, IDS, and FIM could have. CCFF ¶¶ 527, 532, 632, 642, 662, 715-726, 1184. Moreover, the effectiveness of even these limited tools was greatly diminished because LabMD did not implement them appropriately. LabMD failed to update its antivirus software to detect the ever-growing list of new viruses and failed to regularly run or review antivirus scans, limiting any security benefit the out-of-date software provided. CCFF ¶¶ 529-623, 626. LabMD used a firewall that had very limited capability to identify and log potential intrusions; LabMD rarely reviewed those logs and did not properly configure the software to block outsiders from accessing ports into its network. LabMD also did not enable software firewalls on its employees' computers. CCFF ¶¶ 643-657, 1088-1091. And LabMD's manual inspections of employee computers were particularly unlikely to be useful

because they were haphazard and typically occurred only in response to employee complaints about computer performance. CCFF ¶¶ 660-696. The inadequacy of these measures is evidenced by the fact that LabMD failed to discover that its billing manager had P2P software on her computer for over three years. CCFF ¶¶ 691-695.[12]

By failing to prevent, detect, and correct multiple, systemic, and serious security failures, LabMD created a significant risk that the sensitive personal information for over 750,000 consumers would be disclosed without authorization. Consumers, many of whom did not know of LabMD's existence, could not have reasonably avoided this risk, and LabMD could have cured its security vulnerabilities at little or no additional cost. CCFF ¶¶ 1115-1185. Therefore, its data security practices were unfair.

b. The Significant Risk of Concrete Harm Created by LabMD's Data Security Failures Was Magnified When a LabMD Manager Made Sensitive Consumer Data Available for Sharing on the P2P Network

The voluminous evidence regarding LabMD's serious and systemic data security failures more than satisfies Complaint Counsel's burden of showing that the company's practices created a significant risk of concrete harm. The evidence also demonstrates that this significant risk was further magnified when the company's billing manager downloaded LimeWire file-sharing software onto her work computer and designated nearly every file on that computer for sharing on the Gnutella P2P network. LimeWire ran on the manager's computer from 2005 until it was discovered by the company in 2008. CCFF ¶¶ 1399-1400. The record shows that in designating

[12] That LimeWire software was downloaded on the billing manager's computer and ran undetected by the company for three years, CCFF ¶¶ 1363-1364, also evidences the lack of employee training on security. LabMD's Policy Manual, memorialized in 2010, had a "Software Monitoring Policy" that, if enforced, should have discovered LimeWire. CCFF ¶¶ 465-471.

her "My Documents" folder for sharing on LimeWire, the manager made more than 950 files available for users of the Gnutella P2P to download and read.[13] CCFF ¶¶ 1363-1368, 1375-1379. At least one of those files – the 1718 File, containing the sensitive personal information of more than 9,300 consumers – was available for sharing for nearly a year and was accessed and downloaded by at least one unauthorized third party. CX0008-0011, CX0697 (1718 File) (dated June 6, 2007); CCFF ¶¶ 1399 (P2P installed on billing computer in 2005 or 2006); 1364 (LabMD did not detect use of LimeWire prior to May 2008); 1394-1395 (third party downloaded 1718 File; LabMD notified of its availability in May 2008).

In addition to downplaying this fact, the Initial Decision erroneously concludes that the sharing of the 1718 File did not cause or was not likely to cause substantial injury because the only way a third party could discover and download any shared file would be to search for its exact name. In reaching this conclusion, the Initial Decision ignored: (1) persuasive expert testimony that there are other methods by which a third party could identify and obtain the file on the P2P network; and (2) the testimony of a third party who *actually obtained* the 1718 File from the P2P network that indicates that he did not know or search the name of the file prior to obtaining it.

[13] Because LabMD destroyed the billing manager's computer during an attempted forensic examination, the content of the more than 950 documents available for sharing is not known, other than the 1718 File. CCFF ¶ 1409. A screenshot of the sharing folder shows the names of some of the files designated, one of which was named "W-9 Form." CCFF ¶¶ 1375-1377. Employees or contractors provide their SSN or taxpayer identification numbers to employers using this form.

i. The Testimony of Professor Shields Demonstrates the Heightened Significant Risk of Concrete Injury Created by LabMD's Sharing of Patient Files on the P2P Network

In reaching the erroneous conclusion that making the 1718 File available on the Gnutella network did not cause or was not likely to cause substantial injury, the Initial Decision discusses only the risk created by users searching for the terms "insuranceaging" or "6.05.071." ID at 23-24. The Initial Decision ignores the testimony of Complaint Counsel's expert witness Dr. Clay Shields, which established that there are several other ways in which Gnutella users could have located the 1718 File, *see* Shields, Tr. 867-874; CX0738 (Shields Rebuttal Report) ¶¶ 56-76. The Initial Decision disregards this expert testimony even though it is uncontroverted or, as explained below, even supported by LabMD's P2P expert in some instances.[14] *See, e.g.*, Fisk, Tr. 1182-83.

Contrary to the Initial Decision's apparent conclusion that the 1718 File could be found only by someone who knew the exact file name, Dr. Shields's unrebutted testimony established that there were at least three relatively simple ways that P2P users, particularly malicious users, could have located the 1718 File without knowing the file name.

First, Dr. Shields explained that if a user had found any file that was being shared on the LabMD computer, the user could then use LimeWire's built-in browse-host function to view all of the files being shared by the LabMD computer, including the 1718 File. Shields, Tr. at 867-69, CX0738 (Shields Rebuttal Report) ¶¶ 56-58. This testimony was not only uncontroverted, but LabMD's expert agreed. Fisk, Tr. 1182-83. Given that the LabMD billing computer was

[14] Indeed, the Initial Decision cites Dr. Shields's testimony approvingly for other propositions, *see, e.g.*, ID at 22-23, 27 n.19, and makes no credibility findings concerning Dr. Shields. Even if the Initial Decision's failure to consider the complete testimony is taken as a tacit credibility finding, the Commission is equally equipped to judge Dr. Shields's credibility and should consider his complete testimony. *Cf. POM Wonderful LLC*, Docket No. 9344, 2013 FTC LEXIS 6, at *100 n.23 (Jan. 10, 2013) (finding expert credible despite ALJ's contrary conclusions).

sharing more than 950 files, ID at 25 ¶ 86, it is very likely that a Gnutella user could locate one of these files during regular searches. CX0738 (Shields Rebuttal Report) ¶ 59. This is especially true as one of the files being shared was titled "W-9 Form," an IRS form that would be attractive to identity thieves. Shields, Tr. 868; CX0738 (Shields Rebuttal Report) ¶ 58. Any of the millions of Gnutella network users who located any of those files could then use the browse host function to find and download the 1718 File. Shields, Tr. 867-68, 874. A malicious user who found LabMD's computer by searching for other terms would be especially likely to use browse host and examine any files that were likely to contain sensitive personal information, such as a file containing the term "insurance." *See* Shields, Tr. 868.

Second, P2P users could find the 1718 File by searching for particular files that indicate that the sharing computer had been misconfigured to share more than the sharer intended. This method would primarily be implemented by malicious users seeking sensitive information that was being inadvertently shared. Shields, Tr. 868-869; CX0738 (Shields Rebuttal Report) ¶¶ 64-67. Such users would search for files that were commonly installed in computers' main folders, such as the "Windows" or "My Documents" folders. If one of these common files is found in a sharing folder, it is likely that the computer has been misconfigured to share its files broadly, and the malicious user can use the browse host function to explore the shared files, looking for sensitive information. Shields, Tr. 868-869; CX0738 (Shields Rebuttal Report) ¶¶ 64-67.

Finally, P2P users could find the 1718 File by searching for the file extension ".pdf," a search that would yield documents in the Adobe Portable Documents Format, which is commonly used in business environments to distribute documents, and which is more likely to contain sensitive information than other more commonly shared file types, such as music and movies. CX0738 (Shields Rebuttal Report) ¶ 70. Because the 1718 File was saved in this

format, this type of simple search could have found the file. Shields, Tr. 872-873; CX0738 (Shields Rebuttal Report) ¶¶ 68-76.

The risks presented by these simple methods are not speculative. P2P networks are used by malicious individuals who use these simple techniques to seek out sensitive information that has been inadvertently shared. Shields, Tr. 868; CX0738 (Shields Rebuttal Report) ¶ 65. The sheer number of Gnutella users searching the network for files enhances the risk of exposure of sensitive data. Dr. Shields testified that at any given time, the Gnutella network included 2 to 5 million users. Shields, Tr. at 874-75; CX0738 (Shields Rebuttal Report) ¶ 60. With millions of users conducting searches, there was a substantial risk that some of those searches would find the 1718 File and that some of those searches would have been conducted by someone who would misuse the information. Shields, Tr. 873-74; CX0738 (Shields Rebuttal Report) ¶¶ 59-61. Even if it was unlikely that any one search would find the 1718 File, with millions of users on the Gnutella network conducting searches, one would expect the 1718 File to be found many times. Shields, Tr. at 873-74; CX0738 (Shields Rebuttal Report) ¶¶ 59-61. The 1718 File was not on the P2P network for a fleeting instant, but for 11 months of searches conducted by millions of users. If the 1718 File was downloaded from LabMD even once, it could have then been reshared by anyone who had downloaded it, allowing the file to proliferate across the Gnutella network. Shields, Tr. 852-853; CX0738 (Shields Rebuttal Report) ¶¶ 20-22.[15]

[15] The fact that there is no direct evidence of this downloading is unsurprising because LabMD destroyed the billing computer during an attempted forensic examination. CCFF ¶ 1409. If the computer had not been destroyed, a record of any downloads could have been retrieved. Shields, Tr. 863.

ii. LabMD's Own Witness Confirmed the Heightened Significant Risk of Concrete Injury Created by LabMD's Sharing of Patient Files on the P2P Network

The Initial Decision's disregard of Dr. Shields's testimony concerning the methods by which the 1718 File could be located is especially puzzling considering testimony of an individual who located and downloaded the 1718 File, Richard Wallace, whose testimony the Initial Decision specifically held to be credible. Mr. Wallace did not testify that he knew the name of the file before locating it on the Gnutella network, nor did anything in his testimony suggest that it would have been possible for him to have known the file name. Instead, Mr. Wallace testified that he located the 1718 File during a routine search of the P2P network using a stand-alone computer and a standard version of a P2P client. ID at 29, ¶ 122; Wallace, Tr. 1372. There is nothing in his testimony to indicate that he was seeking this particular file at the time, or that he was searching for LabMD's files specifically. Wallace, Tr. 1372. Evidence that Mr. Wallace found and downloaded the file using a standard P2P client as part of a general search for sensitive information demonstrates that any of the millions of other P2P users, and especially those seeking to download and exploit sensitive information, had the opportunity and ability to do the same.

c. The Concrete Harm to Consumers Includes Identity Theft and Medical Identity Theft

As discussed above, the evidence establishes that LabMD's data security failures caused a significant risk of concrete harm to consumers, which was magnified when it made the 1718 File available on a P2P network for nearly a year. *Supra* § VI.B.1.a-b. The record also amply demonstrates that the concrete harms include identity theft and medical identity theft. Kam, Tr. 394; CX0741 (Van Dyke Report) at 3; CCFF ¶¶ 1472-1760..

To describe these types of concrete harm, Complaint Counsel presented expert testimony from Rick Kam and James Van Dyke. The Initial Decision found that Mr. Kam and Mr. Van Dyke have relevant experience and expertise in identity theft and identity fraud. ID at 16-17, ¶¶ 9-10, 12-14. On May 5, 2014, the ALJ denied Respondent's motion in limine to exclude Complaint Counsel's experts. *See* Order Denying Mots. In Limine to Exclude Proffered Experts (May 5, 2014). While, on the basis of unrelated evidentiary findings, the Initial Decision does not credit the entirety of these experts' opinions,[16] *see, e.g.*, ID at 61, it makes no finding that the experts are not qualified or not credible; the Commission should accept and consider their opinions and testimony. *See Sword v. U.S.*, 44 Fed. Cl. 183, 188-89 (1999) ("A fact-finder, especially one with specialized experience . . . can accept or reject opinion testimony, in whole or in part").

The harms consumers experience from identity theft take many forms, including new account fraud, existing card fraud, and existing non-card fraud. CCFF ¶¶ 1479-1484. In addition, consumers who experience these types of fraud will spend considerable amounts of time resolving it. CCFF ¶¶ 1521-1524, 1532-1535, 1544. For example, new account fraud victims spend an average of 26 hours of their own time resolving the fraud. CCFF ¶ 1521. New account fraud is particularly time consuming to resolve because the accounts have been established at institutions with which the victim did not previously have an established relationship. CCFF ¶ 1522.

[16] Complaint Counsel did not rely below nor in this appeal on any of its experts' opinions or testimony predicated on CX0019 or Mr. Boback's testimony, CX0703. *Compare, e.g.*, Complaint Counsel's Post-Trial Brief at 68-71 (not citing Mr. Kam's calculations regarding the likely harm to individuals included in the 1718 File based on the 2013 Ponemon study) *with* Complaint Counsel's Post-Trial Brief at 71-72 (citing Mr. Kam's calculations regarding likely harm to individuals included in the Sacramento Day Sheets based on the 2013 Ponemon Study).

To illustrate that the harms caused by data security failures are undeniably concrete, Complaint Counsel's expert witnesses presented quantified evidence regarding consumers whose sensitive personal information was contained in the Sacramento Day Sheets, as "the most probative indirect evidence . . . available."[17] *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52. These Day Sheets refer to LabMD's electronically-generated reports relating to consumer payments for over 600 consumers, along with copies of checks, that the Sacramento police found at the home of individuals who later pleaded no contest to identity theft. CCFF ¶¶ 150-161, 1714-1719. Complaint Counsel showed that consumers who received notice of the Sacramento Incident in 2013 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

[17] The Initial Decision erroneously concludes that because there was no direct evidence that the Day Sheets had been obtained in digital form from LabMD's network, rather than in paper form, the possession of the Day Sheets by identity thieves does not show that LabMD's data security practices caused consumer injury. ID at 72. The

First, the Initial Decision's reasoning regarding the time frame in which the Day Sheets were digitized represents a misunderstanding of the record. The Initial Decision concluded, based on the deposition of Ms. Nicotra Harris and the investigational hearing of Mr. John Boyle, ID at 39, ¶ 208, that a project to digitize the day sheets and store them on LabMD's computer network had not begun until January 2013, months after the discovery of the Sacramento Day Sheets. ID at 72. However, Ms. Harris testified only that the digitization process was ongoing when she left LabMD in January 2013; she did not indicate when it began or how long it had been proceeding. *See* CX0716 (Harris Dep.) at 25-26. Similarly, Mr. Boyle testified on February 5, 2013 that the project was ongoing and that significant progress had been made. *See* CX0733 (Boyle, IHT) at 37-38, 46-52. He explained that the project involved a LabMD employee scanning 12 years of documents, that the employee was cycling through various kinds of reports, and that the employee had completed scanning three years of billing documents, from 2006 through 2009. *Id*. at 50-51; *see* CX0087 (Day Sheets) (dated 2007-2009). The record does not support the Initial Decision's claim that the project had only begun in January 2013 and, therefore, the conclusion that the Day Sheets could not have been acquired from LabMD's computer network is erroneous.

Second, and most importantly, regardless of the manner in which the Sacramento Day Sheets were obtained, their possession by identity thieves shows that the types of personal information contained on LabMD's network were exactly the types sought by identity thieves.

unauthorized disclosure of the Day Sheets.[18] CCFF ¶¶ 1736-1739, 1742-1746, 1749-1753, 1756-1760. This constitutes 27% of the 600 consumers included in the Day Sheets and copied checks. Consumers will also spend an anticipated 2,497 hours resolving fraud arising from the disclosure of their sensitive information in the Day Sheets. CCFF ¶ 1739.

Consumers also suffer a wide array of harms from medical identity theft, which is a concrete harm associated with the exposure of Social Security numbers, health insurance

[18] Complaint Counsel also offered evidence that Social Security numbers on the Day Sheets were being used by people with different names in CX0451. It was error for the ALJ to have excluded this evidence. *See* ID at 39-41, ¶¶ 213-227. Kevin Wilmer, a Commission investigator, created CX0451 by searching for the Social Security numbers in the Day Sheets in the Consolidated Lead Evaluation and Reporting ("CLEAR") database provided by Thompson Reuters Corporation. ID at 39, ¶¶ 213-221. The CLEAR database, a commercially available law-enforcement database, contains information from a variety of sources, including credit bureaus, utility providers, and information from civil judgments and criminal convictions, and allows a user to determine the names associated with specific Social Security numbers. ID at 39, ¶ 214; Wilmer, Tr. 334-35, 342. Mr. Wilmer determined that approximately 100 of the Social Security numbers found in the Day Sheets had been used by multiple people, which Complaint Counsel's expert opined is an indication of identity theft. CX0742 (Kam Report) at 23 (cited opinion not admitted); CX0451 (not admitted).

The CLEAR Spreadsheet was shown to be both authentic and reliable and should have been considered as evidence, under Commission Rule of Practice 3.43(b). Rule 3.43(b) allows the admission of all relevant, material, and reliable evidence as long as its probative value is not outweighed by the danger of unfair prejudice, or confusion of the issues and the evidence is not misleading. Hearsay evidence, in particular, is admissible if it is relevant, material, and bears satisfactory indicia of reliability. Rule 3.43(b). The CLEAR Spreadsheet meets all these requirements. It is relevant and material to whether consumers whose information was in LabMD's Day Sheets may have become victims of identity theft. *See* CX0742 (Kam Report) at 23. Courts have admitted results from similar databases under Federal Rule of Evidence 803(17), an exception to the hearsay rule that allows the admission of "[m]arket quotations, lists, directories, or other compilations that are generally relied on by the public or by persons in particular occupations." *See, e.g.*, *U.S. v. Woods*, 321 F.3d 361, 364-65 (3d Cir. 2003) (ruling that trial court had properly admitted results of search of database of Vehicle Identification Numbers maintained by the National Insurance Crime Bureau); *U.S. v. Goudy*, 792 F.2d 664, 675-76 (7th Cir. 1986) (affirming trial court admission of results of search from Polk's Bank Directory). The results of Mr. Wilmer's search of the CLEAR database should likewise be admitted in this case.

information, and diagnosis codes.[19] CCFF ¶¶ 1678-1679. Identity thieves specifically target healthcare organizations because of the high value of sensitive medical information. CCFF ¶¶ 1646-1650. Medical identity theft can burden consumers with financial costs related to, among other things, unpaid medical bills from unauthorized procedures and money spent on identity protection, credit counseling, and legal counsel. CCFF ¶¶ 1600-1603. Beyond financial harm, medical identity theft poses serious threats to consumers' health. Consumers may suffer physical harm or even death from misdiagnoses, delays in receiving medical treatment, or unnecessary treatments. CCFF ¶¶ 1612-1618. As with identity theft, consumers spend a significant amount of time resolving problems caused by medical identity theft. CCFF ¶ 1623. Complicating matters, there is no central medical identity bureau where a consumer can set a medical fraud alert, making remediation difficult. CCFF ¶¶ 1627-1630.

2. LabMD's Data Security Failures Caused Injury to Consumers Whose Sensitive Personal Information Was Disclosed Without Authorization in the 1718 File

Consumers whose sensitive personal information is exposed without authorization suffer a loss of privacy, particularly where medical information is exposed. Such a loss of privacy is itself an injury and can result in a constellation of harms that are "substantial and real and cannot

---

[19] The Initial Decision concluded that certain methodological attributes of the 2013 Ponemon Study "detract[ed]" from the Study's reliability. ID at 67. Mr. Kam was not asked during the hearing about the significance of these limitations; in fact, he explained that "many research studies . . . have similar caveats listed." Tr. 541. Indeed, the Commission has indicated that "[t]he methodological design of [survey] research varies significantly and the Commission does not demand perfection, 'but looks to whether such evidence is reasonably reliable and probative.'" *ECM Biofilms, Inc.*, Docket No. 9358, 2015 WL 6384951, at *27 (FTC Oct. 19, 2015) (Comm'n Op.) (citing *POM Wonderful*, Docket No. 9344, 2013 WL 268926, at *45 (Jan. 16, 2013)). There is no evidence or testimony regarding the significance of any of the identified methodological limitations. *See, e.g.*, CCRRFF ¶¶ 403-407 (merely quoting Mr. Kam's testimony); CCRRCL ¶ 184 (citing cases relating to omitted or cherry-picked data, sample size, and cluster sampling, none of which are apposite). Further, the Ponemon Study found that victims of medical identity theft suffered consequences such as misdiagnosis of illness, delay in receiving medical treatment, mistreatment of illness, and having the wrong pharmaceuticals prescribed. CX0742 (Kam Report) at 16. No evidence in the record calls these consequences into question.

fairly be classified as either trivial or speculative." *FTC v Accusearch, Inc*., 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007). Notably, the exposure of one's most sensitive information, including medical information, is an unwarranted intrusion into a consumer's life, and consumers can suffer when information revealing they have a stigmatizing condition is disclosed. CCFF ¶¶ 1606-1609.

In addition to the evidence described above, which shows that it is very likely the 1718 File was accessed by unauthorized third parties, the uncontroverted evidence in this case establishes that it *was* accessed and downloaded by at least one unauthorized third party, Mr. Wallace. Consumers included in the 1718 File have been substantially injured by this disclosure of their sensitive, confidential, personal medical information.[20]

Federal and state statutory law recognize individuals' right to privacy in personal information, particularly medical information. *See, e.g.*, HIPAA, P.L. 104–191 § 264, 110 Stat. 1936 (Aug. 21, 1996) (directing HHS to promulgate a privacy rule for health information); Ga. Code Ann. §§ 31-33-2(d), 31-33-6 (empowering medical providers to keep medical records confidential); Ga. Code Ann. §§ 31-22-9.1(a)(2)(D), 24-12-21(b)(1) (limiting the release of "AIDS confidential information," including that a person a has submitted to an HIV test); Ga. Code Ann. § 24-12-21(o),(u) (imposing criminal liability for intentional or knowing disclosure of AIDS confidential information and permitting civil liability for gross negligence);[21] *see* CX0742 (Kam Report) at 21 & App. D (finding CPT codes indicating HIV tests in 1718 File).

Georgia courts have recognized a right to privacy in medical information since at least 1930. *See Bazemore v. Savannah Hospital*, 155 S.E. 194 (Ga. 1930) (upholding right of parents

[20] The 750,000 consumers whose sensitive personal information is maintained on LabMD's network also face a significant risk of suffering the same injury.

of deceased infant to seek damages for distribution of photographs of infant's deformity). In a case seeking recovery for invasion of privacy in disclosure of plaintiff's HIV positive status, the Georgia Court of Appeals upheld the jury verdict, holding that "invasion of privacy is an action . . . [which] may involve injury to 'the plaintiff's personal sensibilities and mental repose,'" and need not be accompanied by damage to reputation. *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 496 (Ga. Ct. App. 1994) (citing *Hudson v. Montcalm Pub. Corp.*, 379 S.E.2d 572 (1989); *see also Zieve v. Hairston*, 598 S.E.2d 25, 31 (Ga. Ct. App. 2004) (upholding jury verdict on basis that disclosure of cosmetic medical treatment "was one that a reasonable person of ordinary sensibilities would find offensive and objectionable"). A Georgia court has also noted a "qualified right to privacy implicit in the Hippocratic Oath." *Orr v. Sievert*, 292 S.E.2d 548, 550 (Ga. Ct. App. 1982).

The foregoing demonstrates the broad recognition of the inherent harm in the exposure of medical information. The exposure need not result in further injury – the mere disclosure is the harm. Indeed, as described above, Georgia courts have allowed payment of monetary damages to victims whose private data – of a type similar to the data at issue in this case – was exposed. Through its data security failures, LabMD has already imposed this harm on consumers included in the 1718 File whose sensitive personal information exposed includes CPT codes indicating tests for HIV, hepatitis, herpes, prostate cancer, and testosterone levels. CCFF ¶¶ 1684-1697.

---

[21] LabMD is a Georgia corporation and has operated in Georgia at all relevant times. CCFF ¶¶ 54, 66, 68.

VII. CONCLUSION

Complaint Counsel proved that LabMD acted unfairly because its multiple, systemic, and serious security failures caused or were likely to cause substantial injury that consumers could not reasonably avoid, and that this was not offset by countervailing benefits to consumers or competition. LabMD should be adjudged liable under Count 1 of the Complaint based on the record and post-trial briefing submitted to the ALJ, and the Commission should enter the attached order.

Dated: January 14, 2016

Respectfully submitted,

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

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on January 14, 2016, 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 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

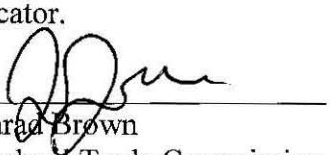
I further certify that I caused a copy of the foregoing document to be served *via* electronic mail to:

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

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.

January 14, 2016 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.

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), 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 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.

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 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.