UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**

OPINION OF THE COMMISSION

By Chairwoman Edith Ramirez, for the Commission:

This case concerns the alleged failure by Respondent LabMD, Inc. to protect the sensitive personal information, including medical information, of consumers whose physicians had entrusted that information to the company. Specifically, Complaint Counsel alleges that LabMD failed to implement reasonable security measures to protect the sensitive consumer information on its computer network and therefore that its data security practices were unfair under Section 5 of the Federal Trade Commission Act. The Administrative Law Judge dismissed the Complaint following an administrative trial, holding that Complaint Counsel had not shown that LabMD's data security practices either caused or were likely to cause substantial injury.

As we explain below, we conclude that the ALJ applied the wrong legal standard for unfairness. We also find that LabMD's security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system. Among other things, it failed to use an intrusion detection system or file integrity monitoring; neglected to monitor traffic coming across its firewalls; provided essentially no data security training to its employees; and never deleted any of the consumer data it had collected. These failures resulted in the installation of file-sharing software that exposed the medical and other sensitive personal information of 9,300 consumers on a peer-to-peer network accessible by millions of users. LabMD then left it there, freely available, for 11 months, leading to the unauthorized disclosure of the information.

We therefore reverse the ALJ's decision and conclude that LabMD's data security practices constitute an unfair act or practice within the meaning of Section 5 of the FTC Act. We enter an order requiring that LabMD notify affected consumers, establish a comprehensive information security program reasonably designed to protect the security and confidentiality of the personal consumer information in its possession, and obtain independent assessments regarding its implementation of the program.

FACTUAL BACKGROUND

From 2001 until early 2014, LabMD operated as a clinical laboratory conducting tests on patient specimen samples and reporting the test results to its physician customers.[1] Once patients' personal information had been downloaded to LabMD's network, physician-clients could order tests and access test results using LabMD's online portal. IDF 46, 50. Over the course of its operations, LabMD collected sensitive personal information, including medical information, for over 750,000 patients. IDF 42-43. This information included names, addresses, dates of birth, Social Security numbers, insurance information, diagnosis codes, and physician orders for tests and services. IDF 44. In many instances, LabMD retrieved the personal information of all of the patients in its physician-clients' databases, regardless of whether LabMD performed tests for those patients. IDF 43.

As discussed in more detail below, from at least 2005 until 2010, LabMD did not have basic data security practices in place for its network. For instance, it had no file integrity monitoring or intrusion detection system in place and did not adequately monitor traffic coming across its firewalls. It failed to provide data security training to its information technology personnel or other employees, in violation of its own internal compliance program. LabMD also lacked a policy requiring strong passwords. For example, at least six employees used "labmd" as their login password.[2] It also failed to take steps to update its software and protect against known vulnerabilities that could be exploited to gain unauthorized access to consumers' personal information.[3]

Additionally, until at least the fall of 2009, management employees were given administrative rights over their workstations and sales employees had administrative rights over their laptop computers. This gave them the ability to change security settings and to download software applications and files of all types from the Internet, many of which – like peer-to-peer ("P2P") file-sharing applications and music files – were unrelated to LabMD's business.

In or about 2005, the P2P file-sharing program LimeWire was downloaded and installed on a computer used by LabMD's billing manager.[4] It was widely known in the billing

---

[1] IDF 24-26. This opinion uses the following abbreviations for citations to the record:
Comp.: Complaint
ID: Initial Decision of the Administrative Law Judge
IDF: Numbered Findings of Fact in the ALJ's Initial Decision
Tr.: Transcript of Trial before the ALJ
CX: Complaint Counsel's Exhibit
RX: Respondent's Exhibit
RAB: Respondent LabMD Inc.'s Corrected Answering Brief
Motion to Dismiss: Respondent LabMD Inc.'s Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings (Nov. 12, 2013)

[2] CX0167; CX0705-A (Bradley dep.) at 125-26.

[3] *See, e.g.*, CX0740 (Hill Expert Report) ¶¶ 70-71, 98-99; CX0731 (Truett dep.) at 81-84.

[4] *See, e.g.*, CX0755 at 4, Response to Interrog. 3; CX0766 at 8-9, Admiss. 40-41; CX0447 at 6-7; CX0150 (Screenshot: C:\) at 1; CX0730 (Simmons dep.) at 10, 24-25.

department that the billing manager and others in the department regularly used LimeWire while at work, primarily for downloading and listening to music.[5]

Often used to share music, videos, and photographs, P2P file-sharing applications allow one computer user to search for and download all files that have been made available for sharing on a "host" computer that is also using the same file-sharing application. IDF 63. LimeWire was one of a number of common P2P applications that used the "Gnutella" P2P protocol.[6] A user shares files on the Gnutella network by designating a directory on his or her computer as a shared directory, making all of the files within the directory freely available for downloading and viewing by other users of the network.[7] Once a file is downloaded by a user from the Gnutella network, the file can be shared further without downloading it again from the original computer. Because of the ease of sharing, it can be extremely difficult or impossible to remove a file from the network once it has been downloaded.[8] Between 2005 and 2010, the Gnutella network had between two and five million users online at any given time.[9]

In February 2008, Richard Wallace, a forensic analyst employed by Tiversa Holding Company, a data security company, discovered and downloaded a copy of one of LabMD's insurance aging reports.[10] Mr. Wallace testified that he used a P2P network and standard P2P application like LimeWire to download the file from a LabMD IP address in Atlanta, Georgia. IDF 121-22. This file, dated June 7, 2007 and referred to as the "1718 file," contained 1,718 pages of sensitive personal information for approximately 9,300 consumers, including their names, dates of birth, social security numbers, "CPT" codes designating specific medical tests and procedures for lab tests conducted by LabMD, and, in some instances, health insurance company names, addresses, and policy numbers. IDF 78, 82. Using the "browse host" function on LimeWire, which enabled him to view all of the shared, downloadable files on LabMD's computer, Mr. Wallace downloaded other documents from the same IP address. IDF 127. Three of these documents also contained sensitive personal information from three consumers, including health insurance data, date of birth, and social security number.[11]

In May 2008, Tiversa, with the aim of obtaining LabMD's business, informed LabMD that the 1718 file had been exposed through LimeWire. IDF 128. Tiversa repeatedly solicited LabMD, offering to sell its breach detection services, and later falsely claimed it had evidence that the 1718 file had spread further across P2P networks.[12]

---

[5] CX0681 at 7; CX0733 (Boyle IH) at 27; CX0730 (Simmons dep.) at 140; CX0716 (Harris dep.) at 86-89, 149; CX0714-A ([Fmr. LabMD Empl.] dep.) at 29-33, 128-31.
[6] IDF 69-71; Shields, Tr. 851.
[7] *See, e.g.*, Shields, Tr. 852; CX0738 (Shields Rebuttal Report) ¶ 17; RX533 (Fisk Expert Report) at 10.
[8] *See, e.g.*, Shields, Tr. 852-54; CX0738 (Shields Rebuttal Report) ¶ 21; CX0740 (Hill Report) ¶ 44.
[9] *See* Fisk, Tr. 1181; RX533 (Fisk Expert Report) at 15; Shields, Tr. 833.
[10] IDF 121-24. Used to track accounts receivable, LabMD's insurance aging reports are spreadsheets documenting insurance claims and payments, and include patients' medical information supporting insurance claims. IDF 52-53.
[11] *Id.*; RX0645 at 39, 42, 43 (*in camera*). We have concentrated our analysis on the much larger 1718 file, but the exposure of sensitive personal information in these additional documents raises concerns similar to those raised by the exposure of comparable information in the 1718 file.
[12] IDF 128-29. In 2009, in response to a request for information from the Commission, a Tiversa affiliate provided the 1718 file to the FTC. IDF 138.

After being contacted by Tiversa, LabMD conducted an internal investigation to determine how the 1718 file had been exposed. IDF 80, 84. It turned out that, during the time that LimeWire had been on the billing manager's computer, the entire contents of her "My Documents" folder had been designated for sharing. IDF 85, 89. Although most of the 950 files in the shared folder were music or videos, the 1718 file and other documents were shared as well. IDF 85-87. Despite clear onscreen warnings from LimeWire that the documents were being shared, neither the billing manager nor anyone else who knew about the P2P file-sharing program did anything to protect the patient information that was being exposed until Tiversa notified LabMD of the disclosure.[13] Once informed of the disclosure, LabMD never notified any of the consumers listed in the 1718 file that their personal information had been disclosed.[14]

Later, in 2010, LabMD hired an independent security firm, ProviDyn, to perform penetration tests on its system and catalogue the vulnerabilities it found. CX0070. ProviDyn identified a number of urgent and critical vulnerabilities on four of the seven servers it tested and rated the overall security of each server as poor. CX0067-CX0071. Among the four servers was the "Mapper" server that LabMD used to receive sensitive information of hundreds of thousands of consumers from physician clients.[15]

Then, in 2012, the Sacramento California Police Department found 40 LabMD "day sheets" containing the names and social security numbers of 600 people, copied checks revealing the names, addresses, and bank numbers of nine individuals, and one money order payable to LabMD (collectively, the "Sacramento documents") while searching the home of individuals suspected of utility billing theft. IDF 182-86, 189-92. The Sacramento Police Department collected the documents as evidence and arrested the two individuals who had possession of the documents; the arrested individuals later pled *nolo contendere* to identity theft. IDF 194-96.

In January 2014, LabMD stopped conducting lab tests and began winding down its business. IDF 36. It continues to preserve tissue samples and provide past test results to healthcare providers. IDF 37, 39. LabMD has not destroyed or deleted any of the patient data it collected. As a result, it continues to maintain the personal data of hundreds of thousands of people on its computer system. IDF 40-42.

PROCEDURAL BACKGROUND

A. The Allegations

On August 28, 2013, the Commission unanimously voted to issue a Complaint against LabMD, alleging that, from 2005 onward, LabMD failed to provide reasonable and appropriate security for personal information stored on its computer network and that its failure caused or

[13] *See* CX0152 (Screenshot: LimeWire: My Shared Files) at 1; CX0154 (Screenshot: LimeWire Get Started) at 1 (screenshots showing warning that the billing computer was sharing numerous files and sub-folders, which could create a security risk); CX0730 (Simmons dep.) at 27-29, 93 (LabMD IT specialist who investigated the 1718 file incident, noting that the billing manager "had no idea what she was doing" when it came to P2P file sharing).
[14] CX0710-A (Daugherty Designee dep.) at 48; Daugherty, Tr. 1087.
[15] CX0725-A (Martin dep.) at 82-83; CX0704-A (Boyle dep.) at 24.

was likely to cause substantial consumer injury, including identity theft, medical identity theft, and other harms, such as the disclosure of sensitive, private medical information. Comp. ¶¶ 10, 12, 22. The Complaint alleges further that LabMD "could have corrected its security failures at relatively low cost using readily available security measures"; that "consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid [these] possible harms"; and that these harms are not offset by countervailing benefits to consumers or competition. *Id.* ¶¶ 11, 12, 22. The Complaint also alleges that LabMD experienced two security breach incidents exposing the 1718 file and possibly other documents containing personal information and the Sacramento documents. *Id.* ¶¶ 17-20. Accordingly, the Complaint alleges that LabMD's security failures constitute an unfair act or practice in violation of Section 5 of the FTC Act, and seeks, among other things, relief requiring LabMD to implement a comprehensive program to protect the security, confidentiality, and integrity of the personal information in its possession. *Id.* ¶¶ 22-23; Comp., Notice Order § I at 7.

LabMD filed its Answer on September 17, 2013. It admitted that LimeWire had been downloaded and installed on a computer used by its billing manager, that it was installed "no later than 2006," and that the 1718 file contains "personal information about approximately 9,300 referring physicians' patients, including names, dates of birth, SSNs, CPT codes, and health insurance company names, addresses, and policy numbers." Ans. ¶¶ 18-19. LabMD denied, or pled insufficient knowledge to admit or deny, most of the other allegations concerning the LimeWire and Sacramento security breach incidents. *Id.* ¶¶ 17-20. LabMD also denied that its security practices were unreasonable or inappropriate and that they violated the FTC Act. Ans. ¶¶ 10, 23.

In addition, LabMD asserted a number of affirmative defenses, including contentions that the Commission lacks statutory authority to regulate the acts or practices alleged in the Complaint; the practices alleged did not cause and are unlikely to cause substantial injury to consumers; and the Commission's alleged failure to provide notice or meaningful standards on data security violates the Fifth Amendment's due process guarantee and the Administrative Procedure Act. *Id.* at 6-7.

B. LabMD's Motions to Dismiss and for Summary Decision

On November 12, 2013, LabMD filed the first of several motions to dismiss the Complaint, arguing that the Commission lacks statutory authority to regulate or bring enforcement actions with respect to data security practices and that the Complaint failed to state a valid claim for relief. The Commission rejected LabMD's jurisdictional arguments and denied the motion on January 16, 2014.[16]

[16] On April 24, 2015, LabMD filed another motion to dismiss, arguing that Complaint Counsel had engaged in "misconduct and indiscretions" in the investigation and prosecution of the case, including its reliance on the evidence provided by Tiversa. The ALJ denied that motion on May 26, 2015. On July 14, 2015, LabMD moved to amend its Answer to add another affirmative defense claiming that the ALJ was not properly appointed under the Appointments Clause of the U.S. Constitution, and then filed another motion to dismiss contending that the FTC's enforcement action was therefore constitutionally defective. The ALJ granted LabMD leave to amend its Answer on July 27, 2015, and we denied the motion to dismiss on September 14, 2015.

On April 21, 2014, LabMD filed a motion for summary decision in which it again raised many of the same jurisdictional challenges and due process arguments it had raised in previous filings. The Commission denied LabMD's motion by order dated May 19, 2014.

C. LabMD's Collateral Attempts to Enjoin the FTC's Enforcement Action

On November 14, 2013, LabMD filed a complaint in the U.S. District Court for the District of Columbia, seeking to enjoin the FTC's enforcement action based on many of the same arguments it had made in its motions to dismiss. A month later, LabMD filed a petition for review in the Eleventh Circuit and moved for a stay of the FTC's administrative proceedings. On February 18, 2014, the Eleventh Circuit dismissed LabMD's petition for lack of jurisdiction. *LabMD, Inc. v. FTC*, Case 13-15267 (11th Cir., Feb. 18, 2014) (*per curiam*). LabMD subsequently withdrew its pending complaint before the D.C. District Court.

In March 2014, LabMD sued for declaratory and injunctive relief in the U.S. District Court for the Northern District of Georgia seeking to enjoin the proceeding before the ALJ and to prohibit the FTC from bringing any further action against it. The district court denied LabMD's motion and granted the FTC's motion to dismiss for lack of subject matter jurisdiction on May 12, 2014. *LabMD, Inc. v. FTC*, 2014 WL 1908716 (N.D. Ga., May 12, 2014). The Eleventh Circuit affirmed on January 20, 2015, concluding that LabMD's arguments are reviewable only after the administrative proceedings are final. *LabMD, Inc. v. FTC*, 776 F.3d 1275, 1277 (11th Cir. 2015).

D. The Evidentiary Hearing

The evidentiary hearing before Chief Administrative Law Judge D. Michael Chappell began on May 20, 2014 and was completed on July 15, 2015.[17]

Complaint Counsel called four expert witnesses. Dr. Raquel Hill, a tenured professor of computer science at Indiana University, was called to assess whether LabMD provided reasonable security for the personal information on its computer networks. Rick Kam, a certified information privacy professional, was asked to assess the risk of injury to consumers resulting from the unauthorized disclosure of sensitive personal information and to describe the types of consumer injuries that occur when firms fail to take reasonable precautions to protect private financial and medical data. James Van Dyke, the founder and President of Javelin Strategy & Research, which conducts survey research on identity theft, assessed the risk of injury to consumers whose personally identifiable information has been disclosed or not adequately protected from unauthorized disclosure. Finally, Dr. Clay Shields, a tenured computer science professor at Georgetown University with special expertise in P2P networks, testified as a rebuttal expert on various issues relating to the functionality of P2P networks and LabMD's exposure of the 1718 file.

[17] Completion of the trial was delayed while Mr. Wallace, the Tiversa forensic analyst who had discovered LabMD's 1718 file, sought to obtain prosecutorial immunity. ID 5.

LabMD called four fact witnesses: Michael J. Daugherty, LabMD's founder and President; Mr. Wallace of Tiversa; Professor Eric Johnson of Dartmouth University, with whom Tiversa shared the 1718 file as part of a research project; and Daniel Kaufman, a deputy director of the FTC's Bureau of Consumer Protection. LabMD also called one expert witness: Adam Fisk, a former lead engineer at LimeWire, who was asked to opine on whether LabMD provided adequate security for the medical information on its computer network.

E. The ALJ's Initial Decision

Judge Chappell issued his Initial Decision on November 13, 2015. He focused on only the first of the unfairness standard's three elements, holding that Complaint Counsel had failed to prove that LabMD's computer data security practices "caused" or were "likely to cause" "substantial consumer injury," as required by Section 5(n) of the FTC Act. On that basis, he dismissed the Complaint.

In so holding, the ALJ defined the phrase "likely to cause" to mean "having a high probability of occurring or being true." ID 54. Applying this standard, the ALJ rejected Complaint Counsel's argument that identity and medical identity theft-related harms were "likely" for consumers whose personal information was maintained on LabMD's computer network. He concluded that, "[a]t best, Complaint Counsel has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm." ID 14.

According to the ALJ, neither the exposure of the 1718 file nor the Sacramento documents incident demonstrated that LabMD's security practices either caused or were likely to cause consumer injury. As to the 1718 file, he rejected Complaint Counsel's argument that the very disclosure of sensitive personal medical information, including lab tests for conditions such as HIV, prostate cancer, and herpes, itself represented substantial consumer injury. He concluded that "[e]ven if there were proof of such harm, this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a 'substantial injury' within the meaning of Section 5(n)." ID 13.

The ALJ also found there was little likelihood of future harm. He explained that Complaint Counsel had not shown that the 1718 file was downloaded by anyone other than Tiversa, and that Tiversa had shared the information only with an academic researcher and the FTC. *See* ID 59-60; IDF 169-81. He concluded that this, combined with the fact that there had been no consumer complaints or injuries linked to the disclosure of the 1718 file, indicated that there was little likelihood that the information in the file would be disclosed to additional individuals or would cause future harm. ID 60.

With respect to the Sacramento incident, the ALJ concluded that Complaint Counsel had failed to establish a causal connection between the incident and any failure of LabMD to reasonably protect data on its computer network as alleged in the Complaint. The ALJ noted that the documents were found in hard copy form and that no evidence had been presented establishing that the documents were maintained on, or taken from, LabMD's computer network. ID 13, 71. Additionally, although the documents were discovered in the possession of identity thieves, the ALJ held that Complaint Counsel had not shown that the exposure of the Sacramento

documents caused or was likely to cause substantial consumer harm. In particular, he highlighted the lack of evidence of consumer complaints or injuries resulting from the incident and reasoned that, because the documents had been booked into evidence by the Sacramento Police Department, there was also no likelihood of future injury. ID 13, 72.

The ALJ declined to address or make any findings of fact with respect to the other issues in the case, including the reasonableness of LabMD's data security practices and the two other unfairness elements – whether the alleged harm was reasonably avoidable by consumers and whether it was outweighed by countervailing benefits to consumers or competition. ID 49, 55-56. He also concluded that, in light of his holding, it was unnecessary to address LabMD's affirmative defenses. ID 14.

Complaint Counsel appeal the ALJ's ruling, arguing that the ALJ misconstrued Section 5(n) by applying an unduly stringent substantial injury standard and failing to recognize that economic and physical harm are not the only forms of cognizable injury. They contend further that he erred by placing undue emphasis on the lack of evidence of particular consumers who suffered actual injury. Complaint Counsel also argue that the ALJ erred by requiring that the probability that consumers will suffer injury be precisely quantified.

LabMD, in turn, urges us to adopt the standard set forth in the ALJ's Initial Decision and affirm his dismissal of the Complaint. As alternative bases for dismissal of the Complaint, LabMD argues that the Commission's unfairness standard is unconstitutionally void for vagueness and fails to provide due process and fair notice. LabMD also claims that dismissal is warranted because the information Complaint Counsel obtained regarding the 1718 file and "all derivative evidence" are based on "unreliable, if not false evidence" provided by Tiversa.

STANDARD OF REVIEW

The Commission reviews the ALJ's findings of fact and conclusions of law *de novo,* considering "such parts of the record as are cited or as may be necessary to resolve the issues presented." 16 C.F.R. §3.54. Our *de novo* review applies to "both findings of fact and inferences drawn from those facts." *McWane, Inc.*, Docket No. 9351, 2014 FTC LEXIS 28, at *30 (Jan. 30, 2014), *aff'd, McWane, Inc. v. FTC,* 783 F.3d 814 (11th Cir. 2015), *cert. denied,* 136 S. Ct. 1432 (2016). We have nonetheless carefully considered the ALJ's factual findings and analysis in the course of conducting our own review.[18]

[18] TechFreedom moved for leave to file an *amicus curiae* brief in support of LabMD. That motion is hereby granted. Most of TechFreedom's arguments are similar to those raised by LabMD, and our discussion of LabMD's arguments incorporates our assessment of TechFreedom's related points. An additional argument TechFreedom raises is that the Commission must defer to the ALJ's Initial Decision absent an abuse of discretion and that the Commission lacks authority to overrule the decision. The contention is meritless. As noted above, the Commission reviews the ALJ's findings *de novo*.

ANALYSIS

I. The Unfairness Standard

Section 5 of the FTC Act authorizes the Commission to challenge "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. §45(a). In 1994, Congress added Section 5(n) to the Act, providing that an act or practice may be deemed unfair if (1) it "causes or is likely to cause substantial injury to consumers"; (2) the injury "is not reasonably avoidable by consumers themselves"; and (3) the injury is "not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). This three-part test, derived from the Commission's 1980 *Policy Statement on Unfairness*,[19] codifies the analytical framework for the Commission's application of its unfairness authority.

Our resolution of this case turns in significant part on the meaning of the first prong of Section 5(n) and the relationships that tie the various elements of the unfairness standard together. In construing and applying Section 5(n), we draw considerable guidance from the *Unfairness Statement* and the many Commission actions and federal court rulings applying the unfairness standard. Within the framework set out by Congress, it is up to the Commission to determine, on a case-by-case basis, which practices should be condemned as "unfair." *See FTC v. Wyndham Worldwide, Inc.*, 799 F.3d 236, 243 (3d Cir. 2015) ("Congress designed the term as a 'flexible concept with evolving content,' and 'intentionally left [its] development . . . to the Commission.'"); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985) (noting the Commission may exercise its discretion to ascertain which "acts or practices . . . injuriously affect the general public" and "to prevent" such acts) (quoting H.R. REP. NO. 75-1613, at 3 (1937)).

The central focus of any inquiry regarding unfairness is consumer injury. *See* FTC, Credit Practices Rule, Statement of Basis and Purpose, 49 Fed. Reg. 7740, 7743 (Mar. 1, 1984) ("*Credit Practices SBP*"), *aff'd, Am. Fin. Servs. Ass'n*, 767 F.2d 957. As reflected in the first prong of Section 5(n), a finding of unfairness requires that the injury in question be "substantial." It is well established that substantial injury may be demonstrated by a showing of a small amount of harm to a large number of people, as well as a large amount of harm to a small number of people.[20] Additionally, in the *Unfairness Statement*, the Commission noted that most cases of unfairness involve economic harm or health and safety risks, and that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair." *Unfairness*

---

[19] *See* FTC, Commission Statement of Policy on the Scope of the Consumer Unfairness Jurisdiction ("*Unfairness Statement*") (Dec. 17, 1980) (*appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984)), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; S. REP. NO. 103-130, at 12-13 (1993) ("SENATE REPORT") (explaining that the amendments were "intended to codify . . . the principles of the FTC's [*Unfairness Statement*]" and to "enable the FTC to proceed in its development of the law of unfairness with a firm grounding in the precedents decided under this authority, and consistent with the approach of the FTC and the courts in the past").

[20] *See* SENATE REPORT at 13; *Unfairness Statement*, 104 F.T.C. at 1073 n.12; *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010) (*quoting Am. Fin. Servs. Ass'n*, 767 F.2d at 972); *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1365 (11th Cir. 1988).

Statement, 104 F.T.C. at 1073. The Commission, however, also recognized that, in extreme cases, subjective types of harm might well be considered as the basis for a finding of unfairness, citing as an example "harassing late-night telephone calls" from debt collectors. *Id*. at 1073 n.16; *see also* SENATE REPORT at 13 (legislative history of Section 5(n) referring to "abusive debt collection practices" and "high pressure sales tactics" as examples of contexts in which the unfairness standard may apply). Indeed, neither the *Unfairness Statement* nor Section 5(n) forecloses the possibility that an intangible but very real harm like a privacy harm resulting from the disclosure of sensitive health or medical information may constitute a substantial injury.

The first prong of Section 5(n) also includes a causation requirement that is satisfied where a practice "causes . . . substantial injury." 15 U.S.C. § 45(n). The practice need not be the only or most proximate cause of an injury to meet this test. As the Third Circuit recently explained in *Wyndham*, "that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms." 799 F.3d at 246.

A practice may also meet the first prong of Section 5(n) if it is "likely to cause substantial injury." Congress therefore expressly authorized the Commission to address injuries that have not yet manifested. *Id.* ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs."). In determining whether a practice is "likely to cause a substantial injury," we look to the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur. Thus, a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low. For example, in *Philip Morris, Inc.*, 82 F.T.C. 16 (1973), the Commission found unfair the unsolicited distribution of free sample razor blades in a manner that could lead the razors to fall into the hands of small children – even though no child had yet been injured. *See also Int'l Harvester Co.*, 104 F.T.C. at 1064 (failure to include a warning label on a tractor gas cap was unfair where the likelihood of harm was low but the injuries were severe). As is the case for analysis of unfairness generally, this evaluation does not require precise quantification. What is important is obtaining an overall understanding of the level of risk and harm to which consumers are exposed. *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 625 (D. N.J. 2014), *aff'd on other grounds*, 799 F.3d 236 (3d Cir. 2015)*; see also Int'l Harvester Co.*, 104 F.T.C. at 1065 n.59; *Am. Fin. Servs. Ass'n*, 767 F.2d at 986; SENATE REPORT at 13.

Under the second and third prongs of Section 5(n), we ask whether consumers could have reasonably avoided the asserted injury and whether it is outweighed by countervailing benefits. *See Unfairness Statement*, 104 F.T.C. at 1073-74; *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1363-64 (11th Cir. 1988) (Commission's "definition of 'unfairness' focuses upon *unjustified* consumer injury") (emphasis added).

Among the types of acts or practices the Commission has long challenged under its unfairness authority are unreasonable and inappropriate data security practices.[21] The Third

[21] To date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases. *See, e.g.*, Commission Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *CardSystems Solutions, Inc.*, FTC File No. 052-3148, Docket No. C-4168 (2006), *available at* https://www.ftc.gov/enforcement/cases-

Circuit succinctly summarized how the three prongs of the unfairness test apply in the data security context in *Wyndham*, describing it as "a cost-benefit analysis" that "considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." 799 F.3d at 255.

This framework dovetails with the analysis the Commission has consistently employed in its data security actions, which is encapsulated in the concept of "reasonable" data security. As the Commission has explained:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. . . . [T]he Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

Commission Statement Marking the FTC's 50th Data Security Settlement, at 1 (Jan. 31, 2014) ("50th Settlement Statement"); *see also* Comm'n Order Den. Mot. to Dismiss at 17-19.

Thus, we evaluate whether LabMD's data security practices, taken together, failed to provide reasonable and appropriate security for the sensitive personal information on its computer network, and whether that failure caused or was likely to cause substantial injury that consumers could not have reasonably avoided and that was not outweighed by benefits to consumers or competition.

We now present an overview of LabMD's data security practices and then apply each of the three prongs of Section 5(n) to the facts here.

II. LabMD's Data Security Practices

LabMD was entrusted with patients' sensitive medical and financial information, and was obligated to put reasonable security systems in place to guard against the risk of an unauthorized release of such information. As discussed below, LabMD did not employ basic risk management techniques or safeguards such as automated intrusion detection systems, file integrity monitoring software, or penetration testing. It also failed to monitor traffic coming across its firewalls. In addition, LabMD failed to provide its employees with data security training. And it failed to

---

proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *Nations Title Agency, Inc.*, FTC File No. 052-3117, Docket No. C-4161 (2006), *available at* https://www.ftc.gov/enforcement/cases-proceedings/052-3117/nations-title-agency-inc-nations-holding-company-christopher; *DSW, Inc.*, 141 F.T.C. 117 (2006); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

adequately limit or monitor employees' access to patients' sensitive information or restrict employee downloads to safeguard the network.

A. LabMD Failed to Protect its Computer Network or Employ Adequate Risk Assessment Tools

Widely known and accepted standards governing minimum reasonable data security practices have long established that risk assessment is an essential starting point. For example, as of 2003, regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat, 1936 (1996), have required covered entities like LabMD that transmit health information to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."[22] While the requirements imposed by HIPAA do not govern whether LabMD met its obligations under Section 5 of the FTC Act, they do provide a useful benchmark for reasonable behavior. Similarly, since at least 2002, National Institute of Science and Technology ("NIST") guidelines provided a framework for risk management for information technology systems that included testing for the presence of vulnerabilities.[23] Additionally, since at least 2005, IT practitioners commonly used intrusion detection systems and file integrity monitoring products to assess whether there were risks on networks.[24] They also used "penetration tests," which are a series of audits that check for conditions such as whether a server's ports are unused and open or whether industry-known software bugs are unpatched, to spot vulnerabilities that criminals could exploit to obtain unauthorized access to sensitive information on the network.[25]

Although LabMD had at least two IT employees on staff,[26] it did none of this. It had no intrusion detection system or file integrity monitoring at all, and it employed penetration testing

---

[22] 45 C.F.R. 164.308 (a)(1)(ii)(A); *see also* CX0405 (HIPAA Security Series) at 1 ("The Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities."). Throughout this proceeding LabMD has acknowledged that it is subject to HIPAA. *See, e.g.*, Motion to Dismiss at 4 ("LabMD's patient-information data-security practices are, and were at all times relevant, regulated under HIPAA and HITECH.").

[23] *See* CX0400 at 17-18 (NIST Special Publication 800-30 (Risk Management Guide for Information Technology Systems) (2002)); *see also* National Research Council, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION (1997) ("NRC Report") (cited as a "comprehensive information security program[] concerning electronic health data," CX0740 (Hill Expert Report) ¶ 60 and n.8) (noting that "[o]rganizations should formally assess the security and vulnerabilities of their information systems on an ongoing basis"), *available at* http://www.nap.edu/catalog/5595.html.

[24] CX0740 (Hill Expert Report) ¶¶ 4, 48, 65, 69 n.22, 104(h). Intrusion detection systems analyze large amounts of network traffic and issue alerts and warnings about threats and suspicious activity. *Id.* ¶ 65. File integrity monitoring products identify changes in critical files that may indicate that malware is present on a network. *Id.*

[25] CX0400 at 24-25; CX0740 (Hill Expert Report) ¶¶ 70-72.

[26] *See, e.g.*, CX0707 (Bureau dep.) at 7; CX0717 (Howard dep.) at 7-11; CX0719 (Hyer dep.) at 46-47, 49; CX0735 (Kaloustian IH) at 7, 13-17; CX0724 (Maire dep.) at 10-11; CX0725-A (Martin dep.) at 9-10; CX0730 (Simmons dep.) at 7. LabMD objects to the introduction of testimony by former LabMD IT employee Curt Kaloustian, arguing that his testimony was obtained during an investigational hearing when LabMD counsel was not present and attorney-client privilege may not have been preserved. LabMD does not identify any particular testimony that purportedly reveals privileged information, and we find no factual basis for LabMD's objection. At the outset of the investigational hearing, the FTC investigator explained that he did not want Mr. Kaloustian "to reveal the content of

only after Tiversa had notified it that the 1718 file was available through LimeWire.[27] The tools that LabMD used to help mitigate risk were antivirus programs, firewall logs, and manual computer inspections, which could identify only a limited scope of vulnerabilities and were often used in a manner that further reduced their effectiveness.[28] For example, LabMD did not consistently update virus definitions[29] or run and review scans.[30] Also, LabMD's manual inspections were not used to detect security risks but merely responded to complaints about computer performance.[31]

LabMD also failed to monitor its network for unauthorized intrusions or exfiltration, which is another common practice long employed by IT professionals.[32] LabMD's firewalls were ineffective for the purpose of risk assessment for two reasons. First, they were not configured properly.[33] Second, no one at LabMD reviewed firewall logs or network activity logs except in connection with troubleshooting a problem, such as with Internet speed or connectivity. For example, there was no attempt to monitor outgoing traffic for items like social security numbers.[34]

One significant consequence of these failures by LabMD was that LimeWire ran undetected on the billing manager's computer between 2005 and 2008.[35] File integrity

---

any communication [he may have] had with an attorney" and offered Mr. Kaloustian the opportunity to proceed only with personal counsel or counsel for LabMD, which Mr. Kaloustian declined. CX0735 (Kaloustian IH) at 9-10. In any event, we rely on Mr. Kaloustian's testimony only for factual descriptions of LabMD's network, equipment, and applications, as well as the day-to-day actions and practices of LabMD's IT employees.

[27] CX0731 (Truett dep.) at 122; CX0717 (Howard dep.) at 58, 140-41; CX0734 (Simmons IH) at 68-69; JX0001-A (Joint Stipulations) at 4; CX0735 (Kaloustian IH) at 92-93.

[28] *See, e.g.*, CX0740 (Hill Expert Report) ¶ 68; CX0735 (Kaloustian IH) at 43-44, 126-27, 187-88.

[29] *See, e.g.*, CX0035 (APT service invoice) at 3; CX0731 (Truett dep.) at 81-84; CX0735 (Kaloustian IH) at 91-92 (many LabMD servers did not receive new virus definitions), 126-32, 160-61 (LabMD relied on individual employees to download new virus definitions from manufacturer websites, but many lacked an internet connection).

[30] LabMD relied on individual employees to run scans, but had no policy requiring them to do so or explaining how and when to conduct the scans. CX0735 (Kaloustian IH) at 126-32. In addition, the Symantec/Norton antivirus program did not automatically report the results of scans to LabMD's IT employees. CX0717 (Howard dep.) at 63-64, 70-71. Thus, LabMD's programs were incapable of determining and revealing whether new viruses had infected the servers and computers. *See* CX0731 (Truett dep.) at 83-84; CX0717 (Howard dep.) at 64-66.

[31] CX0730 (Simmons dep.) at 104, 143-45; CX0707 (Bureau dep.) at 50-51, 89-90.

[32] CX0740 (Hill Expert Report) ¶¶ 65, 68-69(b). This dovetails with HIPAA's requirement that covered entities "[i]mplement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 45 C.F.R. § 164.308(a)(1)(ii)(D).

[33] Although properly configured firewalls should be in place at the network gateway *and* on employee workstations, CX0740 (Hill Expert Report) ¶¶ 31(c), 104(g), until the middle of 2010, LabMD relied only on a ZyWall firewall at the network level. CX0731 (Truett dep.) at 65. The type of network traffic information the ZyWall firewall could record and store was limited, and it could only log information for a few days of traffic. *Id.* at 68-69. Contrary to speculation by LabMD's expert, Mr. Fisk, that LabMD's router could provide significant additional network-level firewall protection, the record shows that, as configured, LabMD's router contributed little to data security. *See, e.g.*, CX0735 (Kaloustian IH) at 96-99; CX0678 at 10; CX0729. The Windows operating system used on the servers also had firewalls available, but LabMD often turned them off. CX0735 (Kaloustian IH) at 293-94.

[34] CX0719 (Hyer dep.) at 167-69. *See also* CX0731 (Truett dep.) at 68-69; CX0717 (Howard dep.) at 98-99; CX0735 (Kaloustian IH) at 115-16. Indeed, the firewall logs were erased by overwriting as frequently as every few days. CX0731 (Truett dep.) at 68-69; CX0710-A (Daugherty, LabMD Designee, dep.) at 176-77.

[35] Ans. ¶ 18(a); CX0755 at 4; CX0447 at 5-6; CX0730 (Simmons dep.) at 54-56; CX0735 (Kaloustian IH) at 269-70; CX0711 (Dooley dep.) at 117-19; CX0443 (LabMD Access Letter Response) at 13.

monitoring or a more complete walk-around inspection could have detected the program, but these safeguards were not in place.[36] Indeed, even after learning of the 1718 file breach in 2008, following which LabMD initiated daily "walk-around inspections," IT employees did not follow any written checklist and instead only asked employees if they were experiencing computer problems.[37]

B. LabMD Failed to Provide Data Security Training to its Employees

Even where basic hardware and software data security mechanisms are in place, there is an increased likelihood of exposing consumers' personal information if employees are not adequately trained. HIPAA's Security Rule, for example, requires that covered entities "[i]mplement a security awareness and training program for all members of [the] workforce (including management)."[38]

LabMD recognized the need for training, as acknowledged in its Compliance Manual which mandated that its compliance officer establish in-house training sessions regarding privacy and security,[39] but it failed to provide such training to any of its employees including its IT personnel.[40] As a result, employees, including sales representatives and billing staff, did not receive training regarding data security, security mechanisms, or the consequences of reconfiguring security settings in applications.[41] For example, the LabMD billing manager from May 2005 to May 2006 testified that she and other billing department employees did not receive any training from LabMD about protecting sensitive health data, stating that LabMD relied on the training that these employees received in their previous employment.[42] Due in part to this lack of data security training, LabMD employees appear not to have understood the risk involved in using P2P file sharing software on LabMD's computers.

C. LabMD Failed to Adequately Restrict and Monitor the Computer Practices of Individuals Using Its Network

LabMD also did not adequately limit or monitor employees' access to the sensitive personal information of patients or restrict employee downloads to safeguard the network.

---

[36] CX0735 (Kaloustian IH) at 92-93; CX0734 (Simmons IH) at 68-69; CX0705-A (Bradley dep.) at 46-47; Hill, Tr. 199-201; CX0740 (Hill Expert Report) ¶ 105; CX0707 (Bureau dep.) at 95-96. *See also* CX0719 (Hyer dep.) at 167-69 (If LabMD had monitored outgoing traffic for items like social security numbers, it could have detected the disclosure of the 1718 file.).

[37] CX0445 at 1-2; CX0730 (Simmons dep.) at 143; CX0719 (Hyer dep.) at 98-99.

[38] 45 C.F.R. §164.308(a)(5)(i). Other IT industry guidance provides: "Organizations should establish education and training programs to ensure that all users of information systems receive some minimum level of training in relevant security practices and knowledge regarding existing confidentiality policies. All computer users should complete such training *before* being granted access to any information systems." NRC Report at 174.

[39] CX0005 (LabMD Compliance Program, effective 2003) at 9.

[40] *See, e.g.*, CX0717 (Howard dep.) at 23-26; CX0711 (Dooley dep.) at 148-49; CX0707 (Bureau dep.) at 37-38, 105-06; CX0719 (Hyer dep.) at 130, 159-62: CX0735 (Kaloustian IH) at 208-20; CX0734 (Simmons IH) at 60-67.

[41] *See, e.g.*, CX0706 (Brown dep.) at 90-94; CX0711 (Dooley dep.) at 147-49; CX0714-A ([Former LabMD Employee] dep.) at 85-88; CX0734 (Simmons IH) at 61-62; CX0735 (Kaloustian IH) at 214-15; CX0708 (Carmichael dep.) at 25-26, 42.

[42] CX0706 (Brown dep.) at 96-98.

As the National Research Council has been emphasizing since 1997, "[p]rocedures should be in place that restrict users' access to only that information for which they have a legitimate need." NRC Report at 170. Similarly, HIPAA requires that covered entities implement policies and procedures for authorizing "access to electronic protected information" and "to prevent those workforce members who do not have access . . . from obtaining access to electronic protected health information." 45 C.F.R. § 164.308(a)(3)(i). LabMD's own 2004 employee handbook acknowledged that sharing health information unnecessarily was illegal and that the company was required to take "specific measures to ensure our compliance with this law."[43]

Yet, LabMD failed to employ adequate measures to prevent employees from accessing personal information not needed to perform their jobs. In fact, LabMD turned off the feature of its laboratory information software, LabSoft, that allowed for distinct access settings for different users. CX0717 (Howard dep.) at 117. Even college students hired on a part-time basis could access patients' medical and other sensitive information. CX0706 (Brown dep.) at 98-102. In addition, LabMD's sales representatives were able to use physician-clients' login credentials to log in to LabSoft, which gave them access to patient information. CX0718 (Hudson dep.) at 73-74, 88-89, 183. Because LabMD had no data deletion policy and never destroyed any patient or billing information it received since it began operating,[44] the amount of information on its network was extensive and included copies of personal checks and credit and debit card account numbers in addition to medical information.[45]

Nor did LabMD adequately restrict or monitor what employees downloaded onto their work computers. Throughout the period at issue, it was widely recognized that downloading unauthorized applications to a computer was dangerous, and P2P programs in particular "presented a well-known and significant risk that files would be inadvertently shared."[46] As the NRC also advised, "Organizations should exercise and enforce discipline over user software. At a minimum, they should . . . limit the ability of users to download or install their own software."[47]

Until at least the fall of 2009, LabMD's management employees were given administrative rights over their workstations and its sales employees had administrative rights

---

[43] CX0001 (LabMD Employee Handbook Rev. June 2004) at 6.
[44] CX0710-A (Daugherty, LabMD Designee, dep.) at 215; CX0733 (Boyle, LabMD Designee, IH) at 39-40; CX0443 at 6; CX0717 (Howard dep.) at 113.
[45] CX0716 (Harris dep.) at 19-25; CX0733 (Boyle IH) at 46.
[46] CX0738 (Shields Rebuttal Report)¶ 49; *see also id*. ¶¶ 40-48; CX0874 (SANS Institute InfoSec Reading Room Peer-to-Peer File-Sharing Networks Security) (2002) at 6; CX0878 (US-CERT - Risks of File-Sharing Technology) (2005) at 1 ("By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data . . . . The availability of this information may increase your risk of identity theft . . . .").
[47] NRC Report at 173; *see also* FTC Staff Report, *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues* (June 2005), *available at* https://www.ftc.gov/sites/default/files/documents/reports/peer-peer-file-sharing-technology-consumer-protection-and-competition-issues/050623p2prpt.pdf (noting the risk of inadvertent file-sharing on P2P platforms and methods for protecting against this risk).

over their laptop computers,[48] which allowed them to change security settings and download software applications and music files from the Internet.[49] LabMD's Policy Manual included a Software Monitoring Policy that stated that users' "'add/remove' programs file will be reviewed for the appropriate applications for the specific user."[50] If followed, this policy would have led to detection of the LimeWire program. CX0740 (Hill Report) ¶ 61(b).

In sum, if LabMD had followed proper data security protocols, LimeWire never would have been installed on the computer used by LabMD's billing manager in the first instance, or it would have been discovered and removed soon after downloading. Instead, LimeWire sat on the billing manager's computer for approximately three years and resulted in the exposure of the 1718 file.[51]

III. LabMD's Data Security Practices Were Unfair in Violation of Section 5(n)

We now turn to whether LabMD's data security practices were unfair within the meaning of Section 5(n). As discussed above, we find that LabMD's lax security practices resulted in the unauthorized sharing of the 1718 file on LimeWire, exposing sensitive medical information of 9,300 consumers to millions of Gnutella users. For the reasons discussed below, we further find that, due to the exposure of the 1718 file, LabMD's data security practices caused and were likely to cause substantial injury that was not avoidable by consumers or outweighed by countervailing benefits and thus that LabMD's data security practices were unfair.

We note that Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument.

---

[48] *See, e.g.*, CX0735 (Kaloustian IH) at 187-89; CX0705-A (Bradley dep.) at 147-49; CX0722 (Knox dep.) at 54-56; CX0719 (Hyer dep.) at 27- 31. In fact, at least until some point in 2005, all LabMD employees used the administrator's user name and password for their credentials. Consequently, all LabMD employees had the ability to exercise administrative rights for their computers, although not all LabMD computers had Internet access. CX0717 (Howard dep.) at 19-20; CX0735 (Kaloustian IH) at 166-72.

[49] CX0714-A ([Former LabMD Employee] dep.) at 38-40; CX0717 (Howard dep.) at 77; CX0735 (Kaloustian IH) at 167; CX0705-A (Bradley dep.) at 148-49.

[50] CX0006 (LabMD Policy Manual) at 18. In addition, LabMD's Employee Handbook stated "Personal internet or e-mail usage in the office is prohibited. . . . Computers in the office are property of LabMD and should only be used for company related reasons." CX0001 (LabMD Employee Handbook Rev. June 2004) at 7.

[51] *See supra* nn.4, 13.

A. LabMD's Data Security Practices Caused and Were Likely to Cause Substantial Injury

1. LabMD's Unauthorized Disclosure of the 1718 File Itself Caused Substantial Injury

We address first whether the unauthorized disclosure of the 1718 file caused actual "substantial injury" to consumers. The ALJ held that "privacy harms, allegedly arising from an unauthorized exposure of sensitive medical information . . . unaccompanied by any tangible injury such as monetary harm or health and safety risks, [do] not constitute 'substantial injury' within the meaning of Section 5(n)." ID 85 n.43. We disagree.

It is undisputed that the 1718 file contained names, dates of birth, social security numbers, insurance company names, policy numbers, and codes for laboratory tests performed, including tests for HIV, herpes, prostate cancer, and testosterone levels. IDF 82. We also know that the file was downloaded by at least one unauthorized third-party – Tiversa – and then shared with an academic researcher.

Complaint Counsel introduced evidence of a range of harms that can and often do result from the unauthorized disclosure of sensitive personal information of the types contained in the 1718 file. One category encompasses economic harms resulting from identity theft and medical identity theft. This includes monetary losses due to financial fraud and time and resources expended by consumers in resolving fraud-related disputes.[52] Medical identity theft associated with data breaches can also result in misdiagnosis or mistreatment of illness, and can thereby harm consumers' physical health and safety.[53] There is no dispute that these economic and health and safety harms fall squarely within the types of injury encompassed by Section 5(n).

Because LabMD never notified any of the consumers identified in the 1718 file that their information had been disclosed, we do not know whether the breach of the 1718 file resulted in actual identity theft, medical identity theft, or physical harm for any of the consumers whose information was disclosed. *See* Daugherty, Tr. 1087; CX0710-A (Daugherty dep.) at 48, 50. We therefore evaluate whether the disclosure of sensitive medical information alone, in the absence of proven economic or physical harm, satisfies the "substantial injury" requirement.

We conclude that the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n). For instance, Complaint Counsel's expert, Rick Kam, testified that disclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm."[54] Mr. Daugherty himself recognized the sensitivity of personal medical data and the gravity of its unauthorized disclosure.[55] In fact, the protection of personal

[52] *See* nn.71-72 and accompanying text, *infra.*
[53] ID 49-50; CX0742 (Kam Expert Report) at 15.
[54] CX0742 (Kam Expert Report) at 21; *see also id*. at 16; Kam, Tr. 411-12.
[55] *See* Daugherty, Tr. 989; CX0710-A (Daugherty Designee dep.) at 45.

health information was seen as part of the service LabMD delivered to its customers, and the company trained its sales representatives to assure physician clients that their data would be maintained on secure servers (despite not following through with such protections).[56] As LabMD's Vice President for Operations noted, it is vital for a lab to protect sensitive patient information.[57]

Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers. The Commission brought its very first data security case against Eli Lilly to address lax security practices that resulted in the inadvertent disclosure of the email addresses of Prozac users.[58] *FTC v. Eli Lilly & Co.*, 133 F.T.C. 763, 767-68 (2002) (complaint and consent order). A more recent example involving sensitive medical information is *GMR Transcription Services*. There we alleged that the failure of GMR's service provider to implement reasonable security measures harmed consumers due to the disclosure of files containing notes from medical examinations on the Internet, which included information about psychiatric disorders, alcohol and drug abuse, and pregnancy loss. *GMR Transcription Services, Inc.*, 2014 WL 4252393, *4 (Aug. 14, 2014) (complaint and consent order).[59] And just last month we announced a settlement with Practice Fusion, a cloud-based electronic health record company, for soliciting consumer healthcare reviews in a manner that we alleged failed to adequately disclose that the reviews would be posted on the Internet. We alleged that these practices resulted in the unauthorized disclosure of some patients' sensitive personal and medical information, including health conditions, medications taken, medical procedures performed, and treatments received. Complaint, *In re Practice Fusion, Inc.*, FTC File No. 142-3039 (June 8, 2015).[60]

There is also broad recognition in federal and state law of the inherent harm in the disclosure of sensitive health and medical information. Section 5(n) expressly authorizes us to look to "established public policies" as additional evidence in support of a determination about whether a practice is unfair, including whether it causes substantial injury, and we do so here.[61] Federal statutes such as HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as well as state laws, establish the importance of maintaining the privacy of medical information in particular. *See, e.g.*, HIPAA, 42 U.S.C. §§ 1320 et seq. (directing HHS to promulgate privacy and security rules for health information); 45 C.F.R. Parts 160 & 164 (privacy, data security, and related rules); HITECH Act, Pub. L. No. 111-5, 123 Stat. 226 (2009), *codified at* 42 U.S.C. §§ 300jj *et seq.*; §§ 17901 *et seq.*, and revisions to 42 U.S.C.

---

[56] CX0704-A (Boyle dep.) at 128-29; CX0718 (Hudson dep.) at 67-68.
[57] CX0704-A (Boyle dep.) at 128-29.
[58] This was brought as a deception case, but still demonstrates the Commission's concern with protecting sensitive medical information.
[59] *Available at* https://www.ftc.gov/enforcement/cases-proceedings/122-3095/gmr-transcription-services-inc-matter.
[60] *Available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3039/practice-fusion-inc-matter.
[61] In highlighting the public policies about sensitive health and medical information established in these laws, we are not saying that practices are unfair simply because they offend those policies. Rather, such laws support our conclusion that the unauthorized exposure of sensitive health and medical information causes substantial consumer injury. *See* 15 U.S.C. § 45(n) ("In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence;" however, public policy considerations may not "serve as a primary basis for [an unfairness] determination").

§§ 1320d—1320d(8); Freedom of Information Act, 5 U.S.C. § 552(b)(6) (restricting agencies from disclosing "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"); Fair Credit Reporting Act, 15 U.S.C. §§ 1681a(i) & 1681b(g)(1) (generally prohibiting reporting agencies from releasing "a consumer report that contains medical information . . . about a consumer" for employment, credit, or insurance purposes)); *id*. § 1681a(i) (defining "medical information"); Ga. Code Ann. § 31-33-2(d) (forbidding release of medical records without patient's signed written authorization); *id.* § 31-22-4(c) (restricting clinical labs' disclosure of test results); *id.* §§ 31-22-9.1(a)(2)(D), 24-12-21(b)(1) (limiting the release of "AIDS confidential information," including the fact that a person has submitted to an HIV test); *id.* § 24-12-21(o), (u) (imposing criminal liability for intentional or knowing disclosure of AIDS confidential information and permitting civil liability for "gross negligence").

Federal courts have similarly acknowledged the importance of protecting the confidentiality of sensitive medical information. *See, e.g.*, *Maracich v. Spears*, 133 S. Ct. 2191, 2202 (2013) (recognizing that an individual's "medical and disability history" is among "the most sensitive kind of information" and characterizing its use in attorney solicitations as a "substantial . . . intrusion on privacy"); *Harris v. Thigpen*, 941 F.2d 1495, 1513-14 (11th Cir. 1991) (expressing view that prison inmates' interest in preventing non-consensual disclosure of their HIV-positive diagnoses, although not absolute, is "significant" and "constitutionally-protected"). State courts, including those in Georgia, also have long recognized a right to privacy in sensitive medical information. *See, e.g.*, *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E. 2d 491 (Ga. App. 1994) (en banc) (affirming verdict awarding damages for public disclosure of AIDS diagnosis).

Tort law also recognizes privacy harms that are neither economic nor physical. As explained by the Restatement of Torts, when "intimate details of [one's] life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy, unless the matter is one of legitimate public interest." RESTATEMENT (SECOND) OF TORTS § 652D, Comment b (1977). Thus, one can be held liable for invasion of privacy if "the matter publicized is of a kind that[:] (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Id.* § 652D (summarizing tort of "publicity given to private life").[62]

We therefore conclude that the privacy harm resulting from the unauthorized disclosure of sensitive health or medical information is in and of itself a substantial injury under Section 5(n), and thus that LabMD's disclosure of the 1718 file itself caused substantial injury.

[62] According to a Comment to this section, "if [a] record is one not open to public inspection, as in the case of income tax returns, it is not public, and there is an invasion of privacy when it is made so." *Id.* at Comment b. The D.C. Circuit has also affirmed the FTC's determination that certain debt-collection techniques are "unfair acts and practices" because they "invade the consumer's right of privacy, causing embarrassment and humiliation," and often harm consumers' reputations for financial stability and degrade their relationships with employers. *Credit Practices SBP*, 49 Fed. Reg. at 7744; *see Am. Fin. Servs. Ass'n*, 767 F.2d at 975 (affirming FTC's adoption of rule and finding such intangible consumer injuries were "neither trivial[,] speculative nor based merely on notions of subjective distress or offenses to taste").

2. LabMD's Unauthorized Exposure of the 1718 File Was Likely to Cause Substantial Injury

We now address whether, independent of our holding that the disclosure of sensitive medical information caused substantial injury under Section 5(n), the unauthorized exposure of the 1718 file for more than 11 months on LimeWire was also "likely to cause substantial injury." The ALJ interpreted "likely to cause" as requiring a showing that substantial consumer injury was "probable." ID 54, 90. He relied principally on the Merriam Webster dictionary's statement that "the word 'likely' is 'used to indicate the chance that something will happen,' and is primarily defined as 'having a high probability of occurring or being true.'" ID 54. On that basis, he concluded that Section 5(n) requires a showing that it is "probable that something will occur," not merely "possible," and that "at best, Complaint Counsel has proven the 'possibility' of harm."[63] ID 14, 54. The ALJ's analysis does not withstand scrutiny.

As an initial matter, we are unpersuaded by the ALJ's reliance on a single dictionary definition to determine the meaning of the phrase "likely to cause" in Section 5(n). Different dictionaries define the phrase differently. *See, e.g.*, Dictionary.com (defining "likely" as "reasonably to be believed or expected"). Some dictionaries define "likely" more broadly when used, as in Section 5(n), with an infinitive ("likely to cause"). Thus, Black's Law Dictionary defines "likely" in the phrase "likely to snow" as "[s]howing a strong tendency; reasonably expected." *Black's Law Dictionary* (10th ed. 2014). Similarly, Collins English Dictionary defines "likely" when used as an adjective as "probable," but when used with an infinitive as "tending to or inclined."[64] None of these dictionary definitions is dispositive. Where there is disagreement about the meaning of an important statutory term, dictionary definitions may not be particularly helpful. *Bullock v. BankChampaign, N.A.*, 133 S. Ct. 1754, 1758 (2014). "It is a fundamental principle of statutory construction (and, indeed, of language itself) that the meaning of a word cannot be determined in isolation, but must be drawn" from the "specific context in which that language is used, and the broader context of the statute as a whole." *Yates v. United States*, 135 S. Ct. 1074, 1082 (internal quotations omitted).

---

[63] LabMD argues for an even higher threshold to assess likely causation, based on law used to determine whether a plaintiff has suffered an "injury in fact" for purposes of Article III standing. The standing doctrine "developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood" by "limit[ing] the category of litigants empowered to maintain a lawsuit in federal court" and, thereby, "prevent[ing] the judicial process from being used to usurp the powers of the political branches." *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016). Standing doctrine has no application here, where the issue is the authority of an executive branch agency to enforce the law, rather than the authority of federal courts to entertain a private party's lawsuit. Similarly, LabMD is wrong when asserting that the Commission must satisfy standing requirements before imposing a cease and desist order. The Commission, as an independent agency within the executive branch, is simply carrying out its duty to "take Care that the Laws be faithfully executed." U.S. Const. art. II, § 3. Indeed, the "injury in fact" prerequisite for standing is particularly inappropriate given Congress' empowerment of the FTC to "tak[e] preemptive action," consistent with "Section 5's prophylactic purpose." *FTC v. Freecom Communications, Inc.*, 401 F.3d 1192, 1203 (10th Cir. 2005).

[64] *See Collins English Dictionary Online, available at* http://www.collinsdictionary.com/dictionary/english/likely.

Unlike the ALJ, we agree with Complaint Counsel that showing a "significant risk" of injury satisfies the "likely to cause" standard.[65] In arriving at his interpretation of Section 5(n), the ALJ found that Congress had implicitly "considered, but rejected," text in the *Unfairness Statement* stating that an injury "may be sufficiently substantial" if it "raises a significant risk of concrete harm." ID 54-55 (citing *Unfairness Statement*, 104 F.T.C. at 1073 n.12). Yet the legislative history of Section 5(n) contains no evidence that Congress intended to disavow or reject this statement in the *Unfairness Statement*. Rather, it makes clear that in enacting Section 5(n) Congress specifically approved of the substantial injury discussion in the *Unfairness Statement* and existing case law applying the Commission's unfairness authority. *See* SENATE REPORT at 12-13; H.R. REP. NO. 103-617, at 12 (1994) (Conf. Rep.).

We conclude that the more reasonable interpretation of Section 5(n) is that Congress intended to incorporate the concept of risk when it authorized the Commission to pursue practices "likely to cause substantial injury." This reading is supported by prior Commission cases applying the unfairness standard, which also teach that the likelihood that harm will occur must be evaluated together with the severity or magnitude of the harm involved. In other words, contrary to the ALJ's holding that "likely to cause" necessarily means that the injury was "probable," a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low. For example, in *International Harvester* – the quintessential unfairness case – the Commission found the failure to include a warning label on a tractor gas cap to be unfair where harmful fuel geysering accidents had occurred at a "rate of less than .001 percent," but the injuries involved included death and severe disfigurement. *Int'l Harvester Co.*, 104 F.T.C. at 1063; *see also Philip Morris*, 82 F.T.C. at 16 (finding unfairness based on severe health hazards without alleging any injuries had yet occurred).

The Third Circuit interpreted Section 5(n) in a similar way in *Wyndham*. It explained that defendants may be liable for practices that are likely to cause substantial injury if the harm was "foreseeable," *Wyndham*, 799 F.3d at 246, focusing on both the "probability and expected size" of consumer harm. *Id*. at 255. This approach is consistent with the standard applied in negligence cases. As described in the Restatement of Torts, a "negligent act or omission may be one which involves an unreasonable risk of harm to another through . . . the foreseeable action of . . . a third person." RESTATEMENT (SECOND) OF TORTS § 302 (1965).

In this case, there was a significant risk of substantial injury. First, there was a high likelihood of harm because the sensitive personal information contained in the 1718 file was exposed to millions of online P2P users, many of whom could have easily found the file. The ALJ's contrary determination that the 1718 file could only have been found by a search of the file's exact name, IDF 77, was in error. Complaint Counsel's expert on the Gnutella network, Dr. Clay Shields, convincingly explained how the 1718 file could have been found through a variety of commonly-used search techniques that would not have required searching for its exact file name or components thereof.

[65] Complaint Counsel also argues that an act or practice that creates a "significant risk of concrete harm" thereby *causes* a substantial injury. We believe the practices in this case creating a significant risk of injury are more properly analyzed under the "likely to cause" portion of Section 5(n).

For instance, Dr. Shields pointed out that malicious users can and do search for P2P users whose computers are misconfigured. CX0738 (Shields Rebuttal Report) at ¶¶ 65-66. As he explained, a computer may be misconfigured to share files that the user does not intend to share, such as all the files in the "My Documents" directory. Shields, Tr. 868. Users do not need to have any information about the names of the files they hope to find; rather, they can look for common files that are placed in particular directories when installed (*e.g.*, in "My Documents"). CX0738 (Shields Rebuttal Report) at ¶ 65. Finding such files suggests a high probability that the computer is misconfigured and is exposing files that the user does not intend to share. *Id.* at ¶ 66. The searcher who locates such a computer can then use LimeWire's "browse host" function – which permits the searcher to see all the files the host computer is sharing, *id*. at ¶¶ 56-57 – to identify and download potentially sensitive files being inadvertently shared. *Id*. at ¶ 66; Shields, Tr. 844-45. "The LabMD computer, which was running LimeWire, would have been vulnerable to being found in this manner." CX0738 (Shields Rebuttal Report) at ¶ 67.

Dr. Shields explained further that these methods, including use of the browse host functionality, were not speculative – that P2P networks are often used by malicious persons who use these types of simple techniques to seek out information that has been inadvertently shared. *Id*. at ¶ 65. A user could have received a search hit for some other file that was present on the billing manager's computer and then used the browse host function to examine and download other files. Dr. Shields explained that because LabMD's billing manager was using LimeWire to download and share popular music that could result in many search hits, her behavior "could easily have led to the 1,718 File being downloaded through browse host." *Id*. at ¶ 57. He continued:

> In addition, the shared folders on [the billing manager's] computer contained other files that might have drawn the interest of potential thieves and could have been found through the basic search. For example, there was a file named "W-9 Form" being shared. A person who was interested in identity theft might have been searching [for] that term to find addresses and Social Security numbers. The browse host function could then be used to view and download the 1,718 File that was contained in the same shared folders.

Id. at ¶ 58.

Dr. Shields' conclusions are borne out by what actually occurred. Mr. Wallace did not discover the 1718 file by searching for its exact name. Rather, he located the 1718 file while conducting a general search for sensitive information on P2P networks, using standard P2P software. Wallace, Tr. 1342-43, 1372, 1440-41; IDF 122. There is nothing in Mr. Wallace's testimony to suggest that he was searching for LabMD files specifically or that he knew – or even could have known – the 1718 file's exact name.

Dr. Shields also opined that "[w]hile it may be unlikely that any random user would choose to download the 1,718 File, this low probability must be balanced against the enormous number of users on the Gnutella system." CX0738 (Shields Rebuttal Report) at ¶ 59. In particular, he quotes the estimate of LabMD's expert, Adam Fisk, that "[a]t any one time on the LimeWire network there would be approximately 2 to 5 million users online," and opines that

"[o]ver an extended period of time, such as weeks or months, even a 1 in 1,000,000 chance of someone downloading the 1,718 file would therefore result in it being downloaded many times." *Id.* at ¶¶ 60-61. Dr. Shields' opinion, in combination with Mr. Wallace's actual experience, is persuasive evidence that LabMD's exposure of the 1718 file and other documents[66] for sharing on the Gnutella network created a significant likelihood that sensitive medical and other information would be disclosed.[67] Indeed, the sensitivity of the data in LabMD's possession made a breach particularly likely to occur. As Complaint Counsel's expert Mr. Van Dyke noted, the types of sensitive personal information found on the 1718 file are very attractive to identity thieves. CX0741 (Van Dyke Expert Report) at 5-6, 12-13.

The ALJ nonetheless discounted Complaint Counsel's evidence that LabMD's practices were "likely to cause" harm in light of what he characterized as the "inherently speculative nature of predicting 'likely' harm." ID 53. He placed great weight on the fact that Complaint Counsel had "not . . . identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security" and concluded that this "undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless 'likely' to occur." ID 52; *see also id.* at 14, 64, 88.

The ALJ's reasoning comes perilously close to reading the term "likely" out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes. This is particularly true in the data security context. Consumers typically have no way of finding out that their personal information has been part of a data breach. CX0742 (Kam Expert Report) at 17; Kam, Tr. 400-02; *see also* ID 52. Furthermore, even if they do learn that their information has been exposed, it is very difficult for identity theft victims to find out which company was the source of the information that was used to harm them absent notification from the company. Kam, Tr. 398-99. Here, given the absence of notification by LabMD, a lack of evidence regarding particular consumer injury tells us little about whether LabMD's security practices caused or were likely to cause substantial consumer injury.[68] Moreover, Section 5 very clearly has a "prophylactic purpose" and authorizes the Commission to take "preemptive action." *FTC v. Freecom Commc'ns*, 401 F.3d 1192, 1203 (10th Cir. 2005).[69] We need not wait for consumers to suffer known harm at the hands of identity thieves.

---

[66] *See* IDF 127 ("Using the 'browse host' function, Mr. Wallace also downloaded 18 other LabMD documents in addition to the 1718 File, three of which contained Personal Information."). One of those documents contained names and passwords of LabMD employees; others contained the names and social security numbers or the names and insurance information for specific patients. *See* Wallace, Tr. 1405; RX645 at 39-43 (*in camera*).

[67] The ALJ found that LabMD had searched P2P networks for other users in possession of the 1718 file and found nothing. IDF 95-97. Neither the ALJ nor LabMD, however, have identified any evidence suggesting that a malicious user who downloaded the 1718 file would further share that file, rather than simply keep it for his or her own malicious use.

[68] Significantly, LabMD typically interacted only with physicians' offices and had no direct dealings with consumers, other than billing when insurance did not pay. Even consumers whose samples were tested by LabMD may not have known that the company was retaining their sensitive personal data. See CX0726 (Maxey dep.) at 78-81; CX0728 (Randolph dep.) at 67.

[69] *See also FTC v. Gratz*, 253 U.S. 421, 435 n.6 (1920) (Brandeis, J., dissenting) ("The purpose of this bill . . . is to seize the offender before his ravages have gone to the length necessary in order to bring him within the law that we

In addition to demonstrating a significant risk of harm in this case, Complaint Counsel also proved that the severity and magnitude of potential harm was high. As noted above, Complaint Counsel's expert witnesses identified a range of harms that can and do result from the unauthorized disclosure of consumers' sensitive personal information of the type maintained by LabMD on its computer network.

Mr. Kam focused on the consumer harms caused by medical identity theft, *i.e.*, the unauthorized use of a consumer's personal health information such as health insurance policy information, test codes, and diagnosis codes, to fraudulently obtain medical services, prescription drugs, or other products or services, or to fraudulently bill health insurance providers.[70] In particular, Mr. Kam reported the results of a Survey on Medical Identity Theft by the Ponemon Institute in 2013, showing the substantial out-of-pocket expenses that medical identity theft victims typically incur, including "reimbursement to healthcare providers for services received by the identity thief"; costs of "identity protection, credit counseling and legal counsel"; and "payment for medical services and prescriptions because of a lapse in healthcare coverage."[71] He observed that victims typically have to spend significant time to resolve problems caused by medical identity theft, and often give up because the process is so difficult and time-consuming. CX0742 at 15. He also noted that because "[t]here is no central 'medical identity bureau' where a consumer can set up a fraud alert, like they can with the credit bureaus," and as a result, "identity thieves can continue to use a consumer's medical identity to commit identity crimes" for long periods of time. *Id.* at 14.

Mr. Van Dyke emphasized that information like names, addresses, and Social Security numbers cannot be readily changed so that, once compromised, these types of personal information can often be used by malicious actors for an extended period and "could result in affected consumers suffering fraud in perpetuity." CX0741 at 5, 12. Mr. Van Dyke also cited data from a survey conducted by his firm, Javelin, showing the average amount of money that identity thieves steal, the average number of hours that victims spend to resolve specific categories of fraud, and the out-of-pocket costs that victims incur in the course of resolving them. *Id.* at 9-11.[72]

In addition, medical identity theft associated with data breaches can result in misdiagnosis or mistreatment of illness, and can thereby harm consumers' physical health and

---

already have.") (quoting 51 CONG. REC. 11455 (July 1, 1914) (statement of Sen. Albert Cummins, co-sponsor of the legislation ultimately enacted as the FTC Act)).

[70] CX0742 at 11-12. The risks of medical identity theft and its potentially serious consequences were well-known during the relevant time frame. *See, e.g.*, *Medical Identity Theft Environmental Scan*, *available at* https://www.healthit.gov/sites/default/files/hhs_onc_medid_theft_envscan_101008_final_cover_note_0.pdf (prepared by Booz, Allen, Hamilton for HHS and ONC for Health Information Technology, Oct. 2008); P. Dixon, *Medical Identity Theft: The Information Crime That Can Kill You*, *available at* https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/.

[71] CX0742 at 15. According to the Ponemon Survey and Mr. Kam, loss of insurance coverage as a result of medical identity theft is a serious problem. *Id*.

[72] Although Mr. Van Dyke bases his report primarily on the Javelin consumer survey conducted in 2013, Javelin has been conducting similar surveys for the past ten years.

safety. ID 49-50; CX0742 at 15. Mr. Kam explained that a "victim of medical identity theft may have the integrity of [his or her] electronic health record compromised if the health information of the identity thief has merged with that of the victim," and that "[t]he resulting inaccuracies may cause serious health and safety risks to the victim, such as the wrong blood type or life-threatening drug allergies." CX0742 at 15; Kam Tr. 426-27. Medical identity theft victims have also reported other types of health and safety harms caused by the theft, such as delay in receiving medical treatment and incorrect pharmaceutical prescriptions. CX0742 at 16. All of these types of harms are cognizable under Section 5(n).

Finally, given that we have found that the very disclosure of sensitive health or medical information to unauthorized individuals is itself a privacy harm, LabMD's sharing of the 1718 file on LimeWire for 11 months was also highly likely to cause substantial privacy harm to thousands of consumers, in addition to the harm actually caused by the known disclosure.[73]

Having found that the unauthorized exposure of the 1718 file created a high likelihood of a large harm to consumers, we conclude that the unauthorized exposure of the 1718 file was "likely to cause substantial injury to consumers."

3. The Sacramento Incident

We do not find, however, that the security incident involving the Sacramento documents provides additional evidence that LabMD's computer security practices caused or were likely to cause substantial injury. LabMD does not dispute that the Sacramento Police Department discovered the documents in the possession of identity thieves. However, unlike with the 1718 file incident, the evidence does not establish any causal link between the exposed documents, which were found in hard copy form, and LabMD's computer security practices.

The fact that the documents were found in the hands of identity thieves strongly suggests that they viewed the information contained therein (including names and social security numbers) as valuable for their purposes. It also raises concerns that LabMD's lax security practices may not have been confined to its computers. Nonetheless, like the ALJ, we conclude that Complaint Counsel have not established that the Sacramento security incident was caused by deficiencies in LabMD's *computer* security practices, which were the sole practices challenged in the Complaint. *See* Comp. ¶ 10.

B. Consumers Could Not Reasonably Avoid the Injuries Resulting from LabMD's Data Security Practices

Turning to the second prong of Section 5(n), we find that consumers had no ability to avoid the harms caused by LabMD's practices. LabMD's clients were physicians or other health care providers. Most patients who provided blood or tissue samples for testing were not notified that their specimens would be given to LabMD for testing, or that LabMD would receive and retain other sensitive personal information as well. CX0726 (Maxey, SUN Designee, dep.) at 78;

[73] *See* nn.54-62 and accompanying text, *supra*.

CX0728 (Randolph, Midtown Designee, dep.) at 67.[74] While some consumers eventually learned of LabMD's existence during the billing or collections process, even these consumers lacked any information about LabMD's data security practices, CX0726 (Maxey, SUN Designee, dep.) at 80-81, 100-01, and thus had no opportunity to avoid injuries caused by these practices. In sum, victims of a LabMD data breach would have "no chance whatsoever to avoid the injury before it occurred." *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008), *aff'd*, 604 F.3d 1150 (9th Cir. 2010).

LabMD nonetheless argues that consumers were reasonably capable of mitigating any injury "after the fact." We disagree. Our inquiry centers on whether consumers can avoid harm *before* it occurs.[75] Second, even assuming *arguendo* that the ability to mitigate harm does factor into its avoidability, there is nothing LabMD has pointed to that demonstrates mitigation after the fact would have been possible here. Without notice of a breach, consumers can do little to mitigate its harms. CX0742 (Kam Expert Report) at 17; Kam, Tr. 398-402. LabMD would be the entity to provide such notice if a breach occurred on its network, yet it did not notify the relevant 9,300 consumers that their medical and other sensitive personal information had been exposed in the 1718 file. CX0710-A (Daugherty Designee dep.) at 48; Daugherty, Tr. 1087. Moreover, even if consumers do receive notice that their information was involved in a breach, it may be difficult or impossible to mitigate or avoid further harm, since they have "little, if . . . any, control over who may access that information" in the future,[76] and tools such as credit monitoring and fraud alerts cannot foreclose the possibility of future identity theft over a long period of time.[77] Furthermore, consumers cannot avoid or fully reverse certain categories of non-economic injury that may accompany the exposure of sensitive medical information. In short, there was no way for consumers to avoid the injury that was caused or likely to be caused by LabMD's inadequate data security practices.

C. The Injuries Were Not Outweighed by Countervailing Benefits to Consumers or to Competition

Finally, we must consider whether the consumer injury resulting from LabMD's data security practices is "outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). A "benefit" can be in the form of lower costs and then potentially lower prices for consumers, and the Commission "will not find that a practice unfairly injures consumers unless it is injurious in its net effects." *Unfairness Statement*, 104 F.T.C. at 1073. This cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk

[74] Moreover, LabMD also holds personal data of approximately 100,000 consumers for whom it never performed tests. JX0001-A (Joint Stipulations) at 3; CX0710-A (Daugherty dep.) at 185-90, 192-93, 198.

[75] *See, e.g., In re Orkin Exterminating Co*., 108 F.T.C. at 366 (holding that "[a]nticipatory avoidance through consumer choice was impossible" when consumers had no "reason to anticipate the impending harm" and respondent did not give most consumers information on "the means to avoid it") (quoted with approval in *Orkin*, 849 F.2d at 1365).

[76] For example, in the case of an unauthorized release of information through a P2P network, "once a file has been shared on a P2P network it can be difficult or impossible to remove it from the network." CX0738 (Shields Rebuttal Report) ¶ 21.

[77] Kam, Tr. at 402; CX0742 (Kam Expert Report) at 22-23.

of such injury. *Int'l Harvester Co.*, 104 F.T.C. at 1064. When a case concerns the failure to provide adequate data security in particular, "countervailing benefits" are the foregone costs of "investment in stronger cybersecurity" by comparison with the cost of the firm's existing "level of cybersecurity." *Wyndham*, 799 F.3d at 255.

Here, we conclude that whatever savings LabMD reaped by forgoing the expenses needed to remedy its conduct do not outweigh the "substantial injury to consumers" caused or likely to be caused by its poor security practices. For the data security failures we described above, the record contains detailed evidence of low-cost solutions that LabMD could have adopted to cure the deficiencies and render its practices reasonable and appropriate. LabMD has not disputed Complaint Counsel's showing as to the availability and cost of these alternatives.

For example, there were many free or low cost software tools and hardware devices available for detecting vulnerabilities, including antivirus programs, firewalls, vulnerability scanning tools, intrusion detection devices, penetration testing programs,[78] and file integrity monitoring tools.[79] CX0740 (Hill Expert Report) ¶ 65. LabMD could have maintained and updated operating systems of computers and other devices on its network at relatively low cost. Hill, Tr. 194; CX0740 (Hill Expert Report) ¶ 101. Remediation processes and updates for vulnerabilities were widely available. CX0740 (Hill Expert Report) ¶ 99. These processes included free notifications from vendors, as well as the Computer Emergency Response Team ("CERT"), the Open Source Vulnerability Data Base, NIST, and others. *Id.*

In addition, LabMD could have adequately trained employees to safeguard personal information at relatively low cost. Hill, Tr. 173-76; CX0740 (Hill Expert Report) ¶ 92. Several nationally recognized organizations provided low-cost or free IT security training courses. Hill, Tr. 173-74; CX0740 (Hill Expert Report) ¶ 89 & n.30. For example, the SysAdmin Audit Network Security (SANS) Institute, formed in 1989, provides free security training webcasts. Additional free resources could be found online, and CERT at Carnegie Mellon University offered e- learning courses for IT professionals for as little as $850. Hill, Tr. 174-75; CX0740 (Hill Expert Report) ¶ 89 n.30.

LabMD also could have limited employees' access to only the types of personal information that they needed to perform their jobs at relatively low cost. Hill, Tr. 166-67; CX0740 (Hill Expert Report) ¶ 85. Because operating systems and applications already have access controls embedded in them, rectifying this issue would have required only the time of trained IT staff. Hill, Tr. 166-67; CX0740 (Hill Expert Report) ¶ 85. In addition, LabMD could have purged the personal information of consumers for whom it never performed testing at

[78] Since 1997, several well-respected and free penetration test and network analysis mechanisms have been available. Examples include Wireshark (released in 1998 under a different name), Nessus (free until 2008), and nmap (released in 1997). Hill, Tr. 162; CX0740 (Hill Expert Report) ¶ 71. When LabMD hired outside IT service provider ProviDyn to conduct penetration tests after the FTC investigation began, in May 2010, the cost for nine tests was $450. CX0044 at 4; CX0048; CX0488 at 4.

[79] LabMD could have implemented SNORT, a respected and widely used intrusion detection system, which has been available at no cost since 1998. CX0740 (Hill Expert Report) ¶¶ 69 n.22, 104(h). Free file integrity monitoring products, such as Stealth and OSSEC, were also available to LabMD during the relevant time period. CX0740 (Hill Expert Report) ¶ 69 n.22.

relatively low cost. This could have been accomplished using LabMD's database applications, and would have required only the time of trained IT staff. Hill, Tr. 164; CX0740 (Hill Expert Report) ¶ 80(b). We recognize that the time of trained IT staff can amount to a real cost, but LabMD already had multiple IT personnel on staff. Any such additional costs would be far outweighed by the likely adverse consequences to consumers of LabMD's lax security practices.

Finally, LabMD readily could have prevented the installation of LimeWire by simply providing the billing manager and other employees non-administrative accounts on their workstations. CX0740 (Hill Expert Report) ¶¶ 85, 104(a). The Windows operating system that LabMD used included this functionality; LabMD could have made use of it with no monetary expense. *Id.*

Consequently, the benefits resulting from LabMD's flawed practices are negligible because the costs to provide the appropriate data security would have been relatively low. The cost-benefit test "is easily satisfied 'when a practice produces clear adverse consequences for consumers that are not accompanied by an increase in services or benefits to consumers or by benefits to competition.'" *Neovi*, 598 F. Supp. 2d at 1116 (quoting *FTC v. J.K. Publications, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000)). That is the case here.

IV. None of LabMD's Affirmative Defenses or Other Objections Has Merit

A. Fair Notice and Due Process

LabMD's First Amended Answer raised six affirmative defenses, most of which we have already addressed in prior rulings or elsewhere in this Opinion.[80] Our discussion here focuses on LabMD's fifth affirmative defense: that this proceeding violates its Fifth Amendment due process rights and the Administrative Procedure Act because the Commission failed to provide adequate notice of what data security practices are required by Section 5. Although we addressed essentially the same arguments and explained why they are meritless in our January 16, 2014 order, LabMD reiterates and expands on them in the present appeal.

First, LabMD contends that our unfairness standard is "void for vagueness," in violation of the Fifth Amendment. As we noted in our January 16, 2014 order, the Supreme Court and courts of appeals have rejected comparable due process challenges on many occasions and affirmed agency and lower court decisions imposing liability for violations of statutes that, like the FTC Act, use broad terms such as "unfair," "unjust," or "unreasonable" to define which practices are prohibited. *See* Comm'n Order Denying Motion to Dismiss at 15. For example,

[80] We rejected LabMD's first, second, and third affirmative defenses – respectively, the failure to state a claim upon which relief can be granted, absence of subject matter jurisdiction, and an absence of statutory authority to regulate the acts or practices alleged – in our January 16, 2014 order. We also rejected LabMD's contention that its acts and practices were not "in or affecting commerce," as defined in Section 4 of the FTC Act. Comm'n Order Denying Motion to Dismiss at 17. LabMD's fourth defense is that the acts or practices alleged in the Complaint do not constitute a violation of Section 5(n). That assertion is addressed throughout this Opinion, in which we analyze the evidence establishing that LabMD's data security practices satisfied each of the elements in Section 5(n). Finally, we rejected LabMD's sixth affirmative defense (challenging the ALJ's role as presiding officer) in our September 14, 2015 order.

courts and agencies often evaluate restraints of trade under Sections 1 and 2 of the Sherman Act, as well as under the FTC Act's prohibition of "unfair methods of competition," 15 U.S.C. §§ 1, 2, 45(a), using a fact-specific "rule of reason." *See, e.g., FTC v. Indiana Fed. of Dentists*, 476 U.S. 447, 457-59 (1986). For over a century, courts have held that this flexible "rule of reason" standard does not violate defendants' due process rights. *See, e.g., Standard Oil Co. v. United States*, 221 U.S. 1, 66-69 (1911). Similarly, courts have held that agencies may, "consistent[] with the obligations of due process," enforce the prohibitions of "unjust" or "unreasonable" rates or practices in various public utility and common carrier regulatory statutes. *See Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968); *see also FPC v. Hope Natural Gas Co.*, 320 U.S. 591, 601-02 (1944); *Verizon Commc'ns, Inc. v. FCC*, 535 U.S. 467, 477, 481 (2002).

LabMD's vagueness challenge relies heavily on *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012), in which the Federal Communications Commission imposed substantial monetary forfeitures on broadcasters for violating a statute that prohibited broadcast "indecency." But *Fox* is distinguishable from this case in a number of important respects. The regulatory action in *Fox*, penalizing broadcasters based on the content of the language in their programs, directly implicated their First Amendment right to free speech. 132 S. Ct. at 2317. No comparable fundamental right is at issue here. LabMD cannot plausibly contend that it had a constitutional right to manage its computer networks in a manner that was likely to expose sensitive personal information to unauthorized third parties. *See Wyndham*, 799 F.3d at 255 (lower level of statutory notice was required because "[S]ection 45(a) does not implicate any constitutional rights") (citing *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982)).

Moreover, in *Fox*, the agency applied a criminal statute, 18 U.S.C. § 1464, and imposed monetary penalties. By contrast, Section 5 of the FTC Act is a civil statute and only injunctive relief is at issue in this case, not criminal or "quasi-criminal" fines. *Wyndham*, 799 F.3d at 255 & n.20 (citing *Flipside*, 455 U.S. at 498-99, and *Ford Motor Co. v. Texas Dept. of Transp.*, 264 F.3d 493, 508 (5th Cir. 2001)). Section 5 therefore is "subject to a less strict vagueness test." *Flipside*, 455 U.S. at 498.

Additionally, in *Fox*, the agency abruptly reversed a more lenient interpretation to which it had adhered for decades, and imposed liability in a manner that "failed to provide . . . fair notice of what is prohibited." 132 S. Ct. at 2318 (internal quotations omitted). The Court has faulted other abrupt changes of policy for similar reasons in other cases. *See, e.g., Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 (2012) (invalidating agency's "interpretation of ambiguous regulations [that] impose[d] potentially massive liability on respondent for conduct that occurred well before that interpretation was announced" – which was "precisely the kind of 'unfair surprise' against which our cases have long warned"); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 146-47 (2000) (overturning rules in part because agency had repeatedly and consistently stated that it lacked authority to regulate tobacco products). By contrast, here the FTC is imposing the same basic data security standard it has consistently articulated for nearly fifteen years.

LabMD challenges this enforcement proceeding next on the ground that the Commission had "not prescribed regulations or legislative rules under Section 5 establishing medical data security standards" before issuing the complaint against LabMD. In our January 16, 2014 order, we noted that "longstanding case law confirm[s] that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue." Comm'n Order Denying Motion to Dismiss at 14 (citing *SEC v. Chenery*, 332 U.S. 194, 201-02 (1947), and *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974)). Indeed, "complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings." *Id.* at 14-15. By the same token, "it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified," and thus "courts and juries [routinely] subject companies to tort liability for violating uncodified standards of care." *Id.* at 16-17.

Fundamentally, Section 5(n) provides reasonably clear and intelligible guidelines for companies to follow in designing their own data security programs. *See Wyndham*, 799 F.3d at 255. As discussed above, the FTC Act simply requires a company that maintains personal information about consumers to assess the risks that its actions could cause harm to those consumers and to implement reasonable measures to prevent or minimize such foreseeable harm.

We provided ample notice to the public of our expectations regarding reasonable and appropriate data security practices by issuing numerous administrative decisions finding specific companies liable for unreasonable data security practices. Our complaints, as well as our decisions and orders accepting consent decrees, which are published on our website and in the Federal Register, make clear that the failure to take reasonable data security measures may constitute an unfair practice. Those complaints, decisions, and orders also flesh out the specific types of security lapses that may be deemed unreasonable.[81] These widely available materials

[81] *See, e.g.*, *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005); *CardSystems Solutions, Inc.*, 71 Fed. Reg. 10686 (FTC, Mar. 2, 2006) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch); *DSW Inc.*, 141 F.T.C. 117 (2006); *Reed Elsevier, Inc.*, (FTC, July 29, 2008) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter); *TJX Companies, Inc.*, (FTC, July 29, 2008) (*available at* http://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter). The FTC has also provided substantial public guidance outside the litigation context. *See* CX0771 at 2 (Press Release: Press Council of Better Business Bureaus, National Cyber Security Alliance, Federal Trade Commission, offer Businesses Tips For Keeping Their Computer Systems Secure (Apr. 2, 2004)) (recommending that businesses "prohibit[] [their] employees from installing file-sharing programs on their computers"); FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2007) (announced in FTC's press release "FTC Unveils Practical Suggestions for Businesses on Safeguarding Personal Information" (Mar. 8, 2007), *available at* https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding) (advising companies, *inter alia*, to "[k]eep sensitive data in your system only as long as you have a business reason to have it"; "[a]ssess the vulnerability of each connection to commonly known or reasonably foreseeable attacks"; "[s]can computers on your network to identify and profile the operating system and open-network services"; "[m]onitor outgoing traffic for signs of a data breach"; and "[t]ake time to explain the rules to your staff, and train them to spot security vulnerabilities"). *See also* 16 C.F.R. Part 314 (FTC standards for safeguarding consumers' financial information, promulgated pursuant to the Gramm-Leach-Bliley Act); 65 Fed. Reg. 54186 (Sept. 7, 2000) (advance notice of proposed rulemaking and request for comment on Part 314 rules); 66 Fed. Reg. 41162 (Aug. 8, 2001) (proposed rule); 67 Fed. Reg. 36484 (May 23, 2002) (final Part 314 rule and Statement of Basis and Purpose).

"constitute a body of experience and informed judgment to which . . . [parties] may properly resort for guidance." *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976). And even though they "are neither regulations nor 'adjudications on the merits,'" they are sufficient to afford fair notice of what was needed to satisfy Section 5(n). *See Wyndham*, 799 F.3d at 257 (citing *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004); *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008); and *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995)). LabMD cannot seriously contend that it lacked notice that its security failures, which led to at least one documented breach of thousands of consumers' sensitive personal information – practices similar to those committed by other companies against which the FTC has taken action – could trigger Section 5 liability.[82]

B. Exclusion of All Evidence as Claimed "Fruit of the Poisoned Tree"

We concur with the ALJ's conclusions that the testimony of Robert Boback, CEO of Tiversa, was not credible or reliable. IDF 160, 166-68; ID 60. In particular, we agree that Mr. Boback's assertion that Tiversa had gathered evidence showing that the 1718 file had spread to multiple Internet locations by means of LimeWire was false and that the document that purported to list Internet locations where the 1718 file had been found (CX0019) was unreliable. IDF 129, 148-49, 153-54; ID 60. Complaint Counsel do not take issue with these conclusions in their appeal. They represent that they have not relied on Mr. Boback's testimony or on CX0019 here or in their pre- or post-trial briefs before the ALJ.

LabMD nonetheless argues that all of the evidence obtained by Complaint Counsel should have been excluded from the record. According to LabMD, Complaint Counsel "knew, or should have known" that Tiversa was not authorized to obtain the 1718 file, that all of Complaint Counsel's evidence was the direct "fruit" of the 1718 file, and thus that the entire case should have been dismissed. RAB 64. This argument fails.

First, the record does not show that Tiversa, whatever its motives, unlawfully obtained the 1718 file; LabMD made the file freely available for public viewing through LimeWire. Moreover, even evidence improperly obtained by private individuals and provided to law enforcement officials is not excluded unless the private actors served as agents of the government. *See, e.g., United States v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990) ("[T]he exclusionary rule of the Fourth Amendment does not apply to a search and seizure by a private person not acting in collusion with law enforcement officials in order to circumvent the requirements of a search warrant.").

As the Court of Appeals for the Eleventh Circuit has explained, "the exclusionary rule is designed to deter police misconduct, rather than to punish the errors of others," so that "[m]isconduct by other actors is a proper target of the exclusionary rule only insofar as those

[82] *See, e.g., BJ's Wholesale Club*, 140 F.T.C. at 467, ¶ 7(4) (2005) (alleging that BJ's "failed to employ sufficient measures to detect unauthorized access or conduct security investigations"); *DSW, Inc.*, 141 F.T.C. at 119, ¶ 7(5) (2006) (alleging that DSW "failed to employ sufficient measures to detect unauthorized access"); Comp. ¶ 10(g) (alleging that LabMD "did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks").

others are adjuncts to the law enforcement team." *United States v. Herring*, 492 F.3d 1212, 1217 (11th Cir. 2007) (internal quotations omitted). Accordingly, the exclusionary rule applies only in "those areas where its remedial objectives [*i.e.*, deterring law enforcement agents from violating the Fourth Amendment] are thought most efficaciously served." *United States v. Calandra*, 414 U.S. 338, 348 (1974). Furthermore, the Supreme Court has made clear that the government does not violate due process by reason of improper private conduct so long as the agency did not "exercise[] coercive power or . . . provide[] such significant encouragement, either overt or covert," to induce the private actors to commit such purportedly unlawful conduct. *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982).

There is no evidence that Tiversa acted as an "agent" or "adjunct" to the FTC in obtaining the 1718 file, much less that anyone at the FTC "exercised coercive power" compelling Tiversa to do so. Consequently, even granting that Tiversa was financially motivated to obtain confidential information, there was nothing improper about Commission staff's receipt of the information via a civil investigative demand in a law enforcement matter.[83]

This case is thus entirely distinguishable from the principal case on which LabMD relies, *Knoll Associates, Inc. v. FTC.*, 397 F.2d 530 (7th Cir. 1968), in which the court concluded that Complaint Counsel's "use of . . . stolen documents render[ed] the Commission's order unenforceable." *Id*. at 533-34. In that case, undisputed evidence showed that a former sales representative had stolen the documents "for the purpose of assisting the Commission counsel in the prosecution of the proceeding," and that Complaint Counsel "knowingly gave its approval to [his] unlawful act." *Id.* at 533. None of those factors is present here. No proceeding against LabMD was pending when Tiversa obtained the 1718 file and nothing in the record indicates that Tiversa was acting at the direction or behest of FTC staff.[84]

[83] LabMD's assertion that the use of the Privacy Institute "as a PHI conduit made the government a party to conduct which violated HIPAA," RAB 64, is unclear. As described in the Initial Decision, the FTC issued its civil investigative demand to the Privacy Institute, a Tiversa affiliate created for the purpose of receiving the CID. IDF 136-38. LabMD does not explain why directing the CID to a Tiversa affiliate, rather than to Tiversa itself, made the FTC a party to a HIPAA violation. We see no factual or logical relationship between the manner in which the FTC staff obtained information from Tiversa and the manner in which Tiversa obtained the information in the first place.

[84] The ALJ found, based on Mr. Wallace's testimony, that after the meeting between Tiversa and FTC staff in the fall of 2009, Mr. Boback directed Mr. Wallace to generate false information purporting to show that the 1718 file had spread to multiple locations on the Internet and could be downloaded from those locations. IDF 146-49. LabMD apparently asks us to infer that FTC staff asked Tiversa to generate such false information in order to use it as evidence against LabMD. However, there is no basis whatsoever for such an inference. At trial, Mr. Wallace thoroughly discussed both his contacts with the FTC and Mr. Boback's directions regarding creation of evidence that the 1718 file had spread to multiple locations. At no time did he suggest that FTC staff knew of, or in any way acquiesced in, Mr. Boback's direction, much less that FTC staff had asked or suggested that such evidence be generated. *See* Wallace Tr. 1347, 1369-70, 1380, 1383-90, 1408-09, 1447. LabMD's related argument – that the FTC knew or should have known that Mr. Boback's testimony was untruthful, so that any continuation of this proceeding violates LabMD's due process rights – is similarly flawed. LabMD presents no factual basis for the assertion that Complaint Counsel knew or should have known that Mr. Boback's testimony was false, and no explanation why continuation of the proceeding *without* continued reliance on Mr. Boback's testimony violates due process.

C. Miscellaneous Objections and Defenses

Over the course of the proceeding, LabMD raised a number of objections to the procedures that the Commission used to conduct this administrative proceeding. None of these objections has merit. First, LabMD challenged the participation of Chief Administrative Law Judge D. Michael Chappell and Chairwoman Edith Ramirez. The Commission rejected both challenges.

Similarly, LabMD argued before the ALJ that the Commission as a whole has infringed LabMD's due process rights because the Commission purportedly has prejudged the outcome of the case. Specifically, LabMD claimed that it was denied due process because there was a "statistical certainty" that the Commission would "find LabMD's data security practices are unfair under Section 5(n) no matter what [the ALJ] does," and that "[t]his clear inevitability of outcome transforms the adjudicatory process into punishment." Resp't's Post-Trial Br. at 58. The argument is meritless. LabMD submitted no evidence that the Commission had "made up [its] mind about important and specific factual questions and [was] impervious to contrary evidence" before deciding this case. *Metro. Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1165 (D.C. Cir. 1995) (internal quotations omitted). Nor did LabMD show that the Commission had "in some measure adjudged the facts as well as the law of a particular case in advance of hearing it." *Cinderella Career & Finishing Sch., Inc. v. FTC*, 425 F.2d 583, 591 (D.C. Cir. 1970) (internal quotations omitted). Rather, as is evidenced by this Opinion, we have decided the contested factual and legal issues on their merits, based on a careful analysis of the record. *Universal Camera Corp. v. NLRB*, 340 U.S. 474, 493, 496-97 (1951); *see also FTC v. Cement Inst.*, 333 U.S. 683, 701-02 (1948) (rejecting claim that FTC's prior conclusions about legal issues denied respondent due process); *Kennecott Copper Corp. v. FTC*, 467 F.2d 67, 79 (10th Cir. 1972) (noting "the courts have uniformly held" that the fact that "the Federal Trade Commission combines the functions of investigator, prosecutor and judge and that Congress designed it in that manner . . . . does not make out an infringement of the due process clause of the Fifth Amendment").

Finally, we find that any defenses or arguments not raised on appeal by LabMD have been waived.[85] *See United States v. Jernigan*, 341 F.3d 1273, 1283 n.8 (11th Cir. 2003) ("a party seeking to raise a claim or issue on appeal must plainly and prominently so indicate"; otherwise, the issue "will be considered abandoned").

[85] In a single sentence in its post-trial brief before the ALJ, LabMD asserted that the FTC violated its First Amendment rights when it issued the Complaint in order "to retaliate against LabMD for speaking out against government overreach." Resp't's Post-Trial Br. 59. Apart from this one sentence, LabMD submitted no explanation of the basis for this argument. The single case LabMD cited in support of this contention, *Trudeau v. FTC*, 456 F.3d 178, 190-91 & n.22 (D.C. Cir. 2006), is inapposite. In that case, the D.C. Circuit affirmed the lower court's dismissal of a party's First Amendment claim against the FTC, but held that the court mistakenly dismissed the case for lack of subject-matter jurisdiction when it should have dismissed it for failure to state a claim. In any case, LabMD has cited no evidence in support of its argument. LabMD has therefore waived any possible First Amendment argument.

V. The Remedy is Appropriate and Required to Prevent Further Consumer Injury

Having found that LabMD violated the FTC Act, we enter an order that will ensure LabMD reasonably protects the security and confidentiality of the personal consumer information in its possession. 15 U.S.C. § 45(b); *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 428 (1957). "The Commission is not limited to prohibiting the illegal practice in the precise form in which it is found to have existed in the past." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 395 (1965) (internal quotations omitted). Rather, "[t]he Commission has wide latitude in fashioning orders to prevent . . . respondents from pursuing a course of conduct similar to that found to have been unfair." *Thompson Med. Co.*, 104 F.T.C. 648, 832-33 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986). This discretion is subject to two constraints, however. First, the order must be sufficiently clear and precise to be understood by the violator. *See, e.g.*, *Colgate-Palmolive*, 380 U.S. at 392. Second, the order must bear a reasonable relationship to the unlawful practice found to exist. *See, e.g.*, *Jacob Siegel Co. v. FTC*, 327 U.S. 608, 612-13 (1946).

We enter an order similar to the Notice Order that was attached to the Complaint. The Order contains three provisions to prevent future violations by LabMD and remediate the risk of harm to consumers.

Part I of the Order requires LabMD to establish, implement, and maintain a comprehensive information security program that is reasonably designed to protect the security and confidentiality of consumers' personal information. The program must be in writing, and should contain administrative, technical, and physical safeguards appropriate to LabMD's size and complexity, the nature and scope of its activities, and the sensitive personal information maintained on LabMD's network. In light of the discussion in our opinion and the availability of guidance about comprehensive information security programs from HIPAA and organizations such as NIST and the SANS Institute,[86] this provision is sufficiently clear and precise that its requirements can be readily understood and met.

Part II of the Order requires LabMD to obtain initial and then biennial assessments and reports regarding its implementation of the information security program. Each assessment must set forth the safeguards that LabMD implemented and maintained during the reporting period and certify that LabMD's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected. The assessments and reports must be provided by a qualified, objective, independent third-party professional. This provision will ensure that LabMD implements information security practices that are appropriate for LabMD's size, complexity, and the nature and scope of its activities and the sensitive personal information maintained on its network, and thereby complies with the Order. Courts have upheld the use of extensive assessment and monitoring requirements by an independent third party in final injunction orders. *See, e.g.*, *United States v. Apple, Inc.*, 992 F.Supp.2d 263 (S.D.N.Y. 2014), *aff'd*, 787 F.3d 131 (2d Cir. 2015).

[86] The FTC also offers guidance. *See, e.g.*, FTC, *Start with Security: A Guide for Business* (2015), *available at* www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

These two provisions are reasonably related to the unlawful practices that form the basis for LabMD's liability – the failure by LabMD to implement reasonable and appropriate data security practices to protect consumers' sensitive medical and other information – and seek to ensure that this failure is remedied. The FTC has required these types of provisions in numerous final orders to settle actions involving data security practices that it charged were violations of Section 5(n). *See, e.g., FTC v. Cornerstone & Co., LLC*, Case No. 1:14-cv-01479-RC, at 5-6, Sec. II (Stip. Final Order for Permanent Inj.) (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc; *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830-RC, at 4-6, Sec. II (Stip. Final Order for Permanent Inj.) (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc.

Part III of the Order requires LabMD to notify individuals whose personal information LabMD has reason to believe was or could have been exposed about the unauthorized disclosure of their personal information. LabMD must also notify the health insurance companies for these individuals of the information disclosure. Without notification, consumers would not know about the unauthorized disclosure of their sensitive information and would not know to take actions to reduce their risk of harm from identity or medical identity theft. LabMD acknowledges that this type of notice is required under HIPAA for disclosures of personal medical information that have occurred since 2010. Daugherty, Tr. 1020-21. Similarly, notice to affected consumers' insurance companies enables these insurers to protect consumers' identities from misuse. These notification requirements are consistent with relief obtained in other cases. *See FTC v. Cornerstone & Co., LLC*, Case No. 1:14-cv-01479-RC, at 7, Sec. IV (Stip. Prelim. Inj.) (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc; *FTC v. Bayview Solutions, LLC*, Case No. 1:14-cv-01830-RC, at 7, Sec. IV (Stip. Prelim. Inj.) (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3226-x140062/bayview-solutions-llc.

The remaining parts of the Order are standard recordkeeping and sunset provisions that are included in most Commission orders. Part IV is a record-keeping requirement. Part V establishes that copies of the Order be distributed to, among others, principals, managers, and employees of LabMD. Part VI requires that LabMD file notifications about changes in corporate structure. Part VII establishes compliance reporting requirements. *See, e.g., FTC v. Direct Mktg. Concepts, Inc.*, 648 F. Supp. 2d 202, 213 (D. Mass. 2009) ("Courts have also included monitoring provisions in final orders in FTC cases to ensure compliance with permanent injunctions."); *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 1013, 1018 (N.D. Ind. 2000) (ordering record retention, notification of changed employment or residence, access to premises, and monitoring); *FTC v. U.S. Sales Corp.*, 785 F. Supp. 737, 753 (N.D. Ill 1992) ("The order should also require Defendants to report their addresses and places of employment or business, and any subsequent changes in this information to the F.T.C."). Part VIII provides that the Order will terminate in 20 years. *See U.S. Sales Corp.*, 785 F. Supp. at 754 (explaining that a complex case "may require a sustained period of monitoring by the F.T.C. to ensure adequate compliance").

Complaint Counsel also seek a provision to require notice to the medical insurance companies for the consumers identified in the day sheets that were recovered in Sacramento.

(LabMD has already provided notice to the individuals whose information was disclosed in the Sacramento incident.) We do not include this provision from the Notice Order that was attached to the Complaint because such relief is not reasonably related to the violation in this case. LabMD's liability is not based on the Sacramento security incident, because we, like the ALJ, conclude that Complaint Counsel have not established that the Sacramento security incident was caused by deficiencies in LabMD's computer security practices. In addition, the day sheets included consumers' names, social security numbers, and copies of personal checks, but did not include medical or insurance information. IDF 182, 183, 185. The absence of medical or insurance information in this unauthorized disclosure provides further reason not to require notice to consumers' medical insurers.

LabMD contends that the relief in the Order is unnecessary and punitive. We disagree. Although LabMD stopped accepting specimen samples and conducting tests in January 2014, LabMD continues to exist as a corporation and has not ruled out a resumption of operations. IDF 36, 40-41; CX0709 (Daugherty dep.) at 15; Daugherty Tr., 1049-54. Moreover, LabMD continues to maintain the personal information of approximately 750,000 consumers on its computer system. IDF 42. Because LabMD continues to hold consumers' personal information and may resume operations at some future time, the Order is appropriate and necessary. *See, e.g., Direct Mktg. Concepts, Inc.*, 648 F. Supp. 2d at 215 (imposing injunction "[e]ven though the . . . defendants currently have no employees and are not engaged in any business, they could resume such activities in the future"); *United States v. Bldg. Inspector of Am., Inc.*, 894 F. Supp. 507, 521 (D. Mass. 1995) (finding injunction appropriate where company had ceased operation but "remains a going concern and could resume at any time"); *cf. Int'l Harvester Co.*, 104 F.T.C. at 1067 ("[A]n obligation should ordinarily extend as long as the risk of harm exists.").

In addition, the Order takes account of LabMD's current limited operations. The Order requires that LabMD establish and implement a comprehensive information security program that provides administrative, technical and physical safeguards that are appropriate for the nature and scope of LabMD's activities. Order, ¶ 1. A reasonable and appropriate information security program for LabMD's current operations with a computer that is shut down and not connected to the Internet will undoubtedly differ from an appropriate comprehensive information security program if LabMD resumes more active operations.

Finally, we reject LabMD's claim that the Order is punitive. The Order merely requires measures reasonably necessary to ensure the protection of the personal information on its computer system and notice related to its unfair practices. An order that is purely remedial and preventative is not a penalty or forfeiture. *See Riordan v. SEC*, 627 F.3d 1230, 1234 (D.C. Cir. 2010).

CONCLUSION

For the foregoing reasons, the Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act. Consequently, we vacate the ALJ's Initial Decision and issue a Final Order requiring that LabMD notify affected individuals, establish a comprehensive information security program, and obtain assessments regarding its implementation of the program.