My LabMD:

1. Find occurences of the word ‘reasonable’ and ‘reasonably’ (and the opposite, unreasonable, or other variations or derivations) in the text, to build the definition…

Count: 27

1a. Find nearest noun or verb that the word reasonable pertains to.

Counts:

Unreasonable security practices - 1

reasonableness: cornerstone of the Commission’s approach to data security – 1

reasonable and appropriate security – 1

minimum reasonable data security practices – 1

reasonable behavior – 1

reasonable security measures – 1

ordinary reasonable man – 1

reasonable person – 1

reasonable interpretation – 1

unreasonable risk of harm – 1

unreasonable data security – 1

**Reasonably Avoid the Injuries – 1**

reasonably capable of mitigating any injury – 1

its practices reasonable and appropriate – 1

the FTC Act, uses broad terms such as “unfair,” “unjust,” or “unreasonable” to define which practices are prohibited – 1

“unjust” or “unreasonable” rates or practices – 1

***reasonable measures- 1***

reasonable and appropriate data security practices – 1

unreasonable data security practices – 1

reasonable data security measures – 1

specific types of security lapses that may be deemed unreasonable – 1

reasonable assurance – 1

reasonable and appropriate data security practices – 1

reasonable and appropriate information security program – 1

measures reasonably necessary – 1

data security practices were unreasonable – 1

1b. Find the most common phrases linked to reasonable to find adjectives and complex noun objects as attributes of reasonableness and identify additional entities which the reasonabless standard applies to.

1c. Identify security controls which are absent, deficient, expected, or recommended.

1d. Identify harms

1e. Identify assets

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.

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

“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.”

**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…

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 definitions29 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 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. 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 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.

**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).

52 *See*

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 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.

§§ 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.

**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 show” 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).

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.

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.

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 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; 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 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 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, 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 “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 ofAll 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 onlyinsofar as those 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

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).

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.

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.*, 141F.T.C. at 119, ¶7(5) (2006) (alleging that DSW“failed to employsufficientmeasures to detect unauthorized access”); Comp.¶10(g) (allegingthat LabMD “did not employ readily availablemeasures to prevent or detect unauthorized access topersonal information on its computernetworks”).

31

- In the Matter of Life is Good, Inc. (2008)

- In the Matter of Petco, Inc. (2005)

- In the Matter of Premier Capital Lending, Inc. (2008)

- In the Matter of Reed Elsevier (2008)

- In the Matter of the TJX Companies, Inc. (2008)

- In the Matter of ValueClick, Inc. (2008)

- United States v. ChoicePoint, Inc. (2006)

- United States v. Google, Inc.

Proposed List of “Reasonable Security” controls:

Classify according to "Program-Level" controls vs. "System-Level" controls.

"Program-Level":

(align with NIST and/or ISO Information Security Management System (ISMS) requirements)

1. Organization of Information Security

2. Risk Management

3. Design, Implementation, and Testing of Safeguards

4. Third Party Oversight

5. Ongoing Monitoring, Review, Maintenance, Development

6. Compliance

"System-Level" controls:

(align with NIST SP 800-53 revision 4 and/or ISO 27001 Annex A controls)

AC- 4 Information Flow Enforcement

AC- 6 Least Privilege

AC- 7 Unsuccessful Login Attempts

AC-18 Wireless Access

IA- 4.b. Unique Identifiers

IA- 5.e. Default Authenticators Changed

IA- 5.g. Change Frequency

IA- 5.h. Authenticator Confidentiality and Integrity

IA- 5 (1) Password-Based Authentication (Internal Users)

IA- 5 (8) Multiple Information System Accounts

RA- 3 Risk Assessment

RA- 5 Vulnerability Scanning

SA-11 Developer Security Testing and Evaluation

SC- 7 Boundary Protection

SC- 7 (10) Prevention of Unauthorized Exfiltration

SC- 7 (13) Isolation of Security Tools / Mechanisms / Support Components

SC- 8 Transmission Confidentiality and Integrity over Untrusted Networks

SC-28 Protection of Information at Rest

SC-28 (1) Cryptographic Protection

SI- 2 Flaw Remediation

SI- 4 Information System Monitoring

Proposed List of *additional* “Reasonable Security” controls:

Custom control enhancements added to a NIST control family have the letter 'C' in front of the control number.

AC-C1 (4) Do Not Store PCI Authentication Data

AT-C2 Role-Based Privacy Training

CO- 3 (2) Other Entity Obligations to Organization

CO- 5 Compliance Review

CO- 5 (1) Scope of Compliance Reviews

IA- 5 (C5) Username Similarities Prohibited

IS- 1 ISMS Policies and Procedures

IS- 2 (2) Inventory of Personally Identifiable Information

IS- 5 Information Security Risk Assessment Process

IS- 6 Information Security Risk Treatment Process

IS- 9 ISMS Personnel Competence

IS-15 Management Review of the ISMS

IS-16 ISMS Continually Improved

PR- 1 Information Privacy Policy and Procedures

PR- 2.c. Personal Data Retention and Disposal

PR- 4 Consent (Choice)

PR- 7 Information Security for Information Privacy [where this is defined

as the 6 'Program-Level" controls in my first list]

PR- 7 (7) Confirmation of an Individual=E2=80=99s Identity

PR- 8 (2) Required Content of Notice

SA- 3 (C2) Development: Secure Coding Practices

Metric: FIPS 199 impact levels of "Low," "Moderate," or "High"

Project: “Evidence-based risk management”

A proposal for "reasonable security wizard"

Create a "wizard-style" web application that asks questions about

context, and then generates an evidence-based list of

"reasonable security practices" that fits that context, along with

strength of evidence.

In this setting, "reasonable security" only has legal meaning and uses. It

is NOT the same as minimum, adequate, "best practice", or desirable

security.

It is not sufficient for decision support in most cases. It is close to

"hygiene" lists, but not identical. (Many hygiene practices are desirable

but not mandatory, b/c redundant with other practices, indirect effects,

etc.)

To me, the most challenging aspect is gathering and coding evidence for

and against any given practice. (It's not enough to find supporting evidence.) By "evidence-based", I mean evidence derived from ground-truth data and not just expert opinion or reasoning.

Q. Did you have an inference calculus in mind?

Our community contribution would be curating evidence and putting together

the rules engine behind the wizard, and also making the strength of

evidence visible in the output.

Because this project doesn't use quantitative risk analysis, it might be

more appropriate under securitymetrics.org than SIRA.

"By "evidence-based", I mean evidence derived from ground-truth data and

not just expert opinion or reasoning."

While Expert opinion can certainly be evidence, for example: as inferences or conclusions made from 'ground-truth data', it obfuscates the underlying evidence adding another error term (opinion).

A 'wizard' would represent the role of expert opinion (artificially),

making inferences from the contextual inputs you give it, according to the

axioms (rules) you provide.

Therefore, expert opinion should not be used as “ground-truth” raw evidence.

Even a CVSS might represent the expert opinion of the CVSS researcher, while specific findings of compromise in a known environment would truly be evidence we could use for risk analysis.

Project: proportionality of expense to security

Project: 'compliant = secure' approach

Problem: "There are a very large number of cyber security scores in use, some are available commercially and through consulting engagements, others are offered through scorecard checklists. There is no market standard and no

consensus around the effectiveness of any particular security score system in predicting the risk of cyber losses in enterprises, although a number of score systems claim to correlate their scores with loss risk."

- Cambridge Centre for Risk Studies,

Project: Measuring help-desk tickets (data source)

Goal: Determine effectiveness of controls

Question: what controls? type of? Method differ by control or control type? What data sources?

Metric: measure help-desk tickets associated with preventative controls to discover answers to these questions: What evidence exists that events are influenced by preventative controls?

Postulate: Administrative/Managerial controls such as identification and variance management influence the effectiveness of preventative controls.

Postulate: Detective and response controls influence the likelihood that small issues become large. Quantify.

Project: Estimate risk (at least the likelihood piece)

Goal: Estimate risk (at least the likelihood piece)

Question:

How can we identify unwanted outcomes (numerators) within an event set or population (denominators)?

Metric:

validate those estimates with measurements and statistical analysis.

Unwanted outcome metrics:

Breach

malware infections

spam.

Unmet control objectives:

- confidentiality, integrity, availability, productivity, and propriety.

event set (state-based?) or population (asset-based?)(denominators):

the organization as a de facto unit in a population of organizations

containing number of servers, websites, binaries, databases, or some other obvious unit

Number of events

set (sequence) of events within which a unwanted occurs.

Example: a compromise due to SQL injection:

database queries,

http posts,

web sessions,

network connections,

* Are these events or assets?

Email messages count

blocked spam messages

other types of unwanted email

four outcomes from our control environment:

- true positives, true negatives, false positives, and false negatives.

Project: SIRA should publish something like this model:

Injury Prevention: What Works? A Summary of Cost-Outcome Analysis for Injury

Prevention Programs (2014 Update)

http://www.childrenssafetynetwork.org/sites/childrenssafetynetwork.org/files

/InjuryPreventionWhatWorks2014Update%20v9.pdf

Project: For the past 4 years, I and my company have performed the descriptive statistical analysis for the NetDiligenceR Cyber Claims Study.

This study is an aggregate analysis of claims data submitted by a number of

insurers. The sample size is small, and the range of claims paid and total

data breach costs is quite broad and heavily skewed by large breaches

(number of records and/or large amounts).

1) There really isn't a huge motivation for insurance carriers to share

their data. I had a conversation a while back with a broker from one of

the Lloyds of London syndicates. He put it like this:

"Let's say I paid $25M last year in cyber claims. In some sense, you could

say that it cost me $25M to obtain the data that I have. These data

represent a real competitive advantage for me. Why should I give the data

away?"

2) There is a company called Verisk Analytics that has been around

since 1971. The Insurance Services Office (yet another ISO) is perhaps the

best known.

Among the many companies Verisk owns, one is of particular relevance to this

discussion - AIR Worldwide.

AIR Worldwide has published a data standard - similar I suppose to the one

Konrads mentioned below. Here's a link:

https://www.air-worldwide.com/Documentation/Cyber-Exposure-Data-Standard/Ind

ex.htm

3) I tend to agree with Kondrads that the insurance folks are a bit too

hung up on what they call "actuarial quality" data. I am not even sure what

they mean when they say that, but it has become increasingly clear to me

that the underwriters and risk managers could benefit from talking with Doug

Hubbard and others who understand that you usually have more data than you

realize and need less than you think you do.

Project: [SIRA] PCI DSS Metrics Project

Extending the GQM work that SIRA has done for the NIST CSF to other frameworks.

Goal: My goal is to at least go through all of the high-level requirements and work through the GQM methodology to identify metrics for any that are actual control implementation and not just wonking on policy.

Question: Would you like to help create or proof this list of metrics?

Metric:

good first run is complete.

Project:

Date: Fri, 11 Mar 2016 13:13:45 -0800

From: Jeff Lowder <jeff.lowder@societyinforisk.org>

Subject: [SIRA] Resurrecting the IRMBOK Meetings

After a long hiatus, I've doubled the size of my team and finally have the

availability to really focus on finally finish version 1.0 of the

Information Risk Management Body of Knowledge (IRMBOK). If you're

interested in participating, please reply to me privately with days and

times (indicate time zone) which work for you and I will be in touch.

Jeff

Project:

I’m hoping you security leaders, risk wonks, and metrics experts might be

willing and able to help with a research project that Jay Jacobs and I

started recently.

A little bit of background for those that aren’t aware: Jay and I started

the Cyentia Institute as a vehicle for advancing cybersecurity knowledge,

practice, and decisions through data-driven research. We’re starting small

and slow, with one or two projects we can handle in addition to our other

professional duties.

Our first - the one we’re inviting you to participate in - is a topic we think is near and dear to the folks on this list.

We will be interviewing metrics/risk SMEs, infosec executives, and board

members to understand how security posture and information risk is viewed,

measured, used, and communicated across the business. We’re particularly

interested in comparing and contrasting perspectives from these different

groups. Our findings will be freely published for the benefit of the

community.

Wanna participate? If so, you have 2 options. Our preferred method is a

live one-on-one interview that takes about 30 minutes (conducted by Yours

Truly). If that’s going to be tough on your schedule between now and the

end of the year, I can send you an online form to knock out at your convenience. Either way, reply to me directly, and we get the ball rolling.

Task: formalizing and quantifying risk statements

Example: Vulnerability Management.

Evidence: Global data clearly indicates that failure to patch in a timely fashion is a leading cause of compromise.

Q. Why the need to go through a formalized risk process to conclude that vulnerabilities should be patched quickly?

A. For many good reasons, including: documenting the risk in a register so others know it was not overlooked, and because not all vulnerabilities can be patched, and because the words “timely” and “quickly” are not sufficiently defined. Overall, we subvert the risk management process by not applying it uniformly to each risk, control, or outcome. Plus, things which appear to be simplistic and obvious, are actually more complex or nuanced.

^ & ^ & ^ & ^ &

MY SIRA Project:

Select a set of IAM controls to monitor user behavior in regard to resource usage.

Try to determine which controls are most effective for detecting normal and abnormal behavior.

Try to determine which combinations of controls are most effective for proving correlation between events as verification that a single control is effective.

Try to determine the range of normal vs abnormal behavior per-user, and per-resource.

Calculate baseline risk levels for each control and/or control set.

Calculate baseline risk levels for each control and/or control set on a per-user basis and per-resource basis.

.Learn how patterns of events differ from expected process which these controls govern to ascertain implementation gaps and how they affect the effectiveness or verification of control(s).

Break outside the population of selected controls, and look for “elevation-of-privilege” events for all users and resources, such as changing permissions on resources, creating new accounts, etc. Use this set to somehow see what we are missing from our original control set population.

The purpose of all this is to determine “coverage” of our risk analysis: Is the scope of our analysis adequate to support our objective?

Q. Suppose I compare the controls on Windows vs Linux per-user. What’s the difference in my risk analysis?

Here’s my Project plan:

1. Create detection control scripts in Powershell and/or Python for Linux and Windows on my Netwrix control set.