**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

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

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

# COMPLAINT COUNSEL'S REPLY BRIEF TO RESPONDENT'S ANSWERING BRIEF

Alain Sheer
Laura Riposo VanDruff
Jarad Brown
Ryan Mehm
Megan Cox

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

Complaint Counsel

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Statutes**



**Legislative History**



**Cases**

**Regulations**



**Administrative Materials**

**Rules**



**Other Authorities**

## RECORD REFERENCE ACRONYMS & ABBREVIATIONS

**CCAB –** Complaint Counsel's Corrected Appeal Brief

**CCCL –** Complaint Counsel's Proposed Conclusions of Law

**CCFF –** Complaint Counsel's Proposed Findings of Fact

**CCPTB –** Complaint Counsel's Post-Trial Brief

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

**CCRRPTB –** Complaint Counsel's Reply to Respondent's Post-Trial Brief

**RAB –** Respondent LabMD, Inc.'s Corrected Answering Brief

**TFA –** *Amicus Curiae* Brief of TechFreedom in Support of the Position of Respondent Counsel

**ID –** Initial Decision

**Witness, Tr. 0000 –** Citations to Trial Testimony

**Tr. 0000 –** Citations to Trial Arguments

**CX0000 –** Complaint Counsel's Exhibit

**RX000 –** Respondent's Exhibit

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

**RX000 (Witness, Dep.) at xx –** Citations to Deposition Testimony

**CX0000 (Witness Report) at xx –** Citations to Expert Reports

**JX0000 (Joint Stips. of Fact, Law, & Authenticity) at xx –** Joint Stipulations of Fact, Law, and Authenticity

## I. INTRODUCTION

LabMD's unfair practices resulted in multiple, systemic, and serious data security failures. *See* CCAB at 24-30. Complaint Counsel proved that through these failures LabMD violated Section 5, because it caused or likely caused substantial injury that was not reasonably avoidable by consumers and not outweighed by the benefits to consumers or competition. In addition to showing that LabMD's poor data security practices themselves caused or were likely to cause substantial injury, Complaint Counsel introduced additional, undisputed evidence of harm: LabMD's exposure of the 1718 File – which contained the sensitive medical and financial information of 9,300 consumers. The 1718 File was exposed on a peer-to-peer ("P2P") network and disclosed to unauthorized third parties. *See* CCAB at 40-41.

Instead of addressing whether its lax data security practices caused or were likely to cause substantial injury, LabMD asks the Commission to require Complaint Counsel to (1) prove that identity thieves obtained information specifically from LabMD and (2) produce evidence of identity theft victims who were able to trace the theft back to LabMD, a company of which many of them would never have heard. LabMD would also require Complaint Counsel to (3) find other P2P users who downloaded the 1718 File. Recognizing that this type of ex-post analysis of injury may be impossible in many cases, Congress allowed the FTC to prove a violation of Section 5(n) based on an ex-ante analysis of conduct that causes or is likely to cause injury, a burden that Complaint Counsel has more than met in this case.

Respondent's argument, however, would eviscerate the Commission's ability to protect consumers from harm through unfair conduct. Analyzing unfair practices as of the time they occurred provides appropriate incentives to a firm to forego harmful conduct, rather than merely to remedy it after the fact. Indeed, Congress charged the Commission with a broad mandate to

"*prevent* such acts or practices which injuriously affect the general public." Comm'n Order Denying Mot. to Dismiss at 4 (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess., 3 (1937)) (emphasis added).

Complaint Counsel has met its burden and requests that the Commission reverse the Initial Decision, conduct a *de novo* review of the record, find that LabMD violated Section 5 of the FTC Act, and enter the notice order attached to Complaint Counsel's appellate brief.

## II. THE COMMISSION EXERCISES *DE NOVO* REVIEW IN THIS PROCEEDING

Contrary to Respondent's assertion, RAB at 10-12, the Commission reviews the ALJ's findings of facts and conclusions of law *de novo*, exercising "all the powers which it could have exercised if it had made the initial decision." 16 C.F.R. § 3.54; *McWane, Inc.*, Docket No. 9351, 2014 FTC LEXIS 28, at *29-30 (Jan. 30, 2014) (*de novo* review applies to "both findings of fact and inferences drawn from those facts"), *aff'd McWane, Inc. v. FTC*, 783 F.3d 814 (11th Cir. 2015); *POM Wonderful LLC*, Docket No. 9344, 2013 FTC LEXIS 6, at *100 n.23 (Jan. 16, 2013) (finding expert testimony credible despite contrary ALJ findings because ALJ findings were not based on observations of the witness's demeanor but on perceived weaknesses in the expert's experience or methodology), *aff'd Pom Wonderful, LLC v. FTC*, 777 F.3d 478 (D.C. Cir. 2015); *Realcomp II, Ltd.*, Docket No. 9320, 2009 FTC LEXIS 250, at *9 n.4, *37 n.11 (Oct. 30, 2009) (specifically rejecting ALJ inferences and conclusions regarding expert testimony as "faulty and unsound"), *aff'd Realcomp II, Ltd. v. FTC*, 635 F.3d 815 (6th Cir. 2011). There is no support for the notion that the ALJ, once his appointment was ratified by the Commission, assumed greater powers than those originally granted by Congress and set forth in 16 C.F.R. §§ 1 *et seq*. *Cf.* TFA at 14-15.

## III. THE COMMISSION HAS AUTHORITY TO ENFORCE THE FTC ACT BY ADJUDICATING WHETHER DATA SECURITY PRACTICES ARE UNFAIR

### A. Section 5(n) Provides Fair Notice of Its Requirements

Section 5(n) provided LabMD with fair notice of its obligations to secure consumers' sensitive data, as the Commission and the Third Circuit Court of Appeals have previously held. Comm'n Order Denying Resp't's Mot. to Dismiss at 15-17 (Jan. 16, 2014); *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247-49 (3d Cir. 2015) (considering and rejecting claim that Section 5(n) cannot be applied in data security context). The unfairness definition in the FTC Act, 15 U.S.C. § 45(n), "is sufficient to give fair notice of what conduct is prohibited." Comm'n Order Denying Resp't's Mot. to Dismiss at 16; *see also FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 619 (D.N.J. 2014) *aff'd*, 799 F.3d 236 (3d Cir. 2015) (rejecting the contention that regulations are the only means to provide fair notice and stating that "Section 5 codifies a three-part test that proscribes whether an act is 'unfair'"); *Wyndham*, 799 F.3d at 255 (finding that the unfairness "standard informs parties that the relevant inquiry here is a cost-benefit analysis"). Indeed, the cost-benefit standard required by Section 5(n) is routinely used to evaluate legal obligations. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 17. ("LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence.").[1] As a civil statute that regulates economic activities, Section 5(n) provides fair notice of its requirements. *See Wyndham*, 799 F.3d at 250 (quoting *CMR D.N. Corp. v. Philadelphia*, 703 F.3d 612, 631-32 (3d Cir. 2013)); *see also Leib v. Hillsborough Cty.*

[1] Amicus TechFreedom relies on the Third Circuit's decision in *Wyndham* to argue that the FTC must establish "ascertainably certain" standards. TFA at 16-17. This argument is a misreading of *Wyndham*, which expressly rejected the application of this test, holding instead that Section 5(n) must be "not so vague as to not be a rule or standard at all." *Wyndham*, 799 F.3d at 251-52. The court concluded that the FTC Act easily meets this test. *Id.* at 255.

*Pub. Transp. Comm'n*, 558 F.3d 1301, 1310 (11th Cir. 2009) ("Indeed, a civil statute is unconstitutionally vague only if it is so indefinite as really to be no rule or standard at all." (citation and quotation marks omitted)).

Nor is the Commission required to promulgate rules relating to data security before enforcing Section 5 in the data security context, as Respondent contends. RAB at 32; *see* Comm'n Order Denying Resp't's Mot. to Dismiss at 14-15; *Wyndham*, 10 F. Supp. 3d at 619; *see also SEC v. Chenery Corp.*, 332 U.S. 194, 202-03 (1947) (holding that agencies "must be equipped to act either by general rule or *by individual order*" and "retain power to deal with [] problems on a case-to-case basis if the administrative process is to be effective" (emphasis added)).[2] Furthermore, the Commission provides guidance to business and consumers, *see e.g.*, CCFF ¶¶ 1340-1345, and has issued "many public complaints and consent agreements" that "'constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*.'" *Wyndham*, 10 F. Supp. 3d at 620-21 (quoting *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis added by court)); *Wyndham*, 799 F.3d at 257 (noting that courts "regularly consider materials that are neither regulations nor 'adjudications on the merits'" in reviewing fair notice claims).

---

[2] Respondent's reliance on *FCC v. Fox Television Stations, Inc.* is misplaced. RAB at 13-14. *Fox* concerned the retroactive application of a changed agency policy. 132 S. Ct. 2307, 2318 (2012) ("[The FCC's] lack of notice to Fox and ABC that *its interpretation had changed* so the fleeting moments of indecency contained in their broadcasts were a violation . . . 'fail[ed] to provide a person of ordinary intelligence fair notice of what is prohibited.'" (emphasis added; citation omitted)). Here, the Commission "has repeatedly affirmed its authority to take action against unreasonable data security measures as 'unfair . . . acts or practices' in violation of Section 5 . . . [and] has also confirmed this view by bringing administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal information collected from consumers online." Comm'n Order Denying Resp't's Mot. to Dismiss at 8.

### B. HIPAA and Other Statutes Do Not Shield LabMD from Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act

Respondent contends that Section 5 cannot be applied to entities in the medical industry, including those subject to HIPAA.[3] *See, e.g.*, RAB at 13-17, 47-48. HIPAA's requirements are irrelevant to this proceeding, a point LabMD conceded in its discovery responses. *See* CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22 (stating that information regarding whether LabMD complied with HIPAA regulations is "neither relevant nor reasonably calculated to lead to the discovery of admissible evidence").

As the Commission has already recognized, there is no separate standard under Section 5 for medical data security. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 12; *see also* Comm'n Order Denying Resp't's Mot. for Summ. Decision at 5-6 (May 19, 2014). Courts have upheld Section 5's prohibition of "unfair . . . acts or practices" as a flexible prohibition that applies *across* industries. *See, e.g., FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972) (trading stamps); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (televised commercial for shaving cream); *FTC v. Motion Picture Advert. Serv. Co.*, 344 U.S. 392 (1953) (unfair methods of competition in exclusive film-screening agreements); *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010) (online check-processing); *FTC v. Accusearch Inc.*, 570 F.3d 1187 (10th Cir. 2009) (online sale of phone records). Regardless of the industry in which a company operates, the Commission assesses whether a company's data security measures cause or are

[3] Respondent's reference to Mr. Sheer's opening statement for the proposition that the FTC case is based on a "HIPAA statutory standard which was applicable to the LabMD medical data security practices," *see* RAB at 14-15, strains credulity. Mr. Sheer unambiguously stated in his opening that "[t]he evidence will show that LabMD's security practices were unfair under section 5 of the FTC Act." Tr. 11.

likely to cause harm that is not reasonably avoidable by consumers and not outweighed by the benefits to consumers and competition. 15 U.S.C. § 45(n).

Respondent claims the opinions of Complaint Counsel's data security expert Dr. Raquel Hill should be accorded no weight because they did not focus on medical data security or HIPAA. Dr. Hill provided expert testimony relating to computer security and information technology for exactly the type of data LabMD holds. Hill, Tr. 234-35; CX0740 (Hill Report) at 64-66. This information – including names, dates of birth, Social Security numbers, and financial account numbers, JX0001-A (Joint Stips. of Fact, Law, & Authenticity) at 1-2 – is held by organizations operating in many industries. Dr. Hill took into account recommendations, guidelines, and best practices from a wide variety of organizations across industries, including recommendations, guidelines, and best practices on how to protect medical data. CX0740 (Hill Report) at 62-66; Hill, Tr. 234-35; RX524 (Hill, Dep.) at 61-62.

In any event, despite baldly asserting that it complied with HIPAA, LabMD has never shown such compliance, and it refused to provide evidence of such compliance. CX0765 (LabMD's Resps. to Second Set of Discovery) at 12-13, Resp. to Interrog. 22; *see also* Comm'n Order Denying Resp't's Mot. for Summ. Decision at 5 ("LabMD points to no record evidence regarding what measures, if any, it implemented to prevent data breaches. It does not explain which HIPAA standards apply to LabMD's actions or why LabMD's conduct satisfied them."). Its only "evidence" is an unattributed statement, alleged to be from HHS, regarding the FTC's investigation. RAB at 16-17. The quoted language comes from a proposed exhibit, RX649, that was expressly excluded from the evidentiary record, *see* Order on Resp't's Mot. to Admit Exs. at 2 (July 15, 2015), a fact Respondent does not reveal in its brief. RAB at 17. The proposed exhibit is hearsay – a blind quote in a blog post by a pseudonymous blogger – and not probative.

*See infra* § VI.C at 37. It is also irrelevant because it does not support the proposition for which Respondent cites it, as it relates only to the lack of breach notification requirements under HIPAA before the implementation of HITECH, 45 C.F.R. § 164.403-414.[4]

## IV. SECTION 5 AUTHORIZES THE COMMISSION TO PROTECT CONSUMERS FROM ACTS OR PRACTICES THAT CAUSE OR ARE LIKELY TO CAUSE SUBSTANTIAL INJURY

### A. Section 5(n) Contains the Requirements Needed to Establish Unfairness

To prove that LabMD violated Section 5, Complaint Counsel needs to show that LabMD's data security failures caused or were likely to cause substantial injury, were not reasonably avoidable by consumers, and were not outweighed by the benefits to consumers or competition. The clear weight of precedent establishes that this test, codified in Section 5(n) of the FTC Act, contains the requirements for unfairness, notwithstanding the Third Circuit's *dicta* that Section 5(n) could be interpreted as setting forth "necessary, rather than sufficient," criteria.[5] *Wyndham*, 799 F.3d at 259. Thirty years ago in *American Financial*, the D.C. Circuit dismissed a similar argument – that proving unfairness required something more than what was contained in the Unfairness Statement – holding: "the consumer injury test is the *most precise definition of*

---

[4] Respondent suggests that Complaint Counsel relies on HITECH in analyzing LabMD's failure to notify consumers regarding the 1718 File. RAB at 16. To the contrary, Complaint Counsel's statement regarding notification relates to Section 5(n)'s reasonably avoidable factor: consumers could not reasonably avoid harms about which they did not know, such as identity theft. CCAB at 4.

[5] *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010), is even less persuasive authority for this proposition. TFA at 10. The court in *LeBlanc* was interpreting the Fair Debt Collection Practices Act ("FDCPA"), which does not define "unfair," unlike Section 5(n). There, it referred in *dicta* to *dicta* in an earlier FDCPA case, *Jeter v. Credit Bureau, Inc*., 760 F.2d 1168, 1172-75 (11th Cir. 1985). *Jeter* concerned deceptive actions in debt collection, not unfair actions, and it is therefore unsurprising that the *Jeter* court cited the "tendency or capacity to deceive" definition.

*unfairness* articulated by either the Commission or Congress."[6] *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) (emphasis added). *See also* S. Rep. No. 103-130, 1993 WL 322671, at *12 (1993) (Section 5(n) is "intended to codify" the Unfairness Statement, which "itself is based on the FTC's decided cases and rules"); Unfairness Statement, *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *317-18 (rejecting factor of whether conduct was "immoral, unethical, oppressive, or unscrupulous"); *Int'l Harvester Co.*, Docket No. 9147, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *243 (1984) (finding unfairness even in the absence of "a deliberate act on the part of the seller"), *id.* at *247 n.43 ("[T]he theory of immoral or unscrupulous conduct was abandoned altogether."). In adopting Section 5(n) to codify the Unfairness Statement, as described in detail below, Congress imposed no additional restriction on the types of prohibited practices. Indeed, Respondent's argument that Complaint Counsel must prove something more contradicts the very statutory text and structure, and ignores clear judicial precedent. *See*, *e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010); *Am. Fin. Servs. Ass'n*, 767 F.2d 957.

### B. Acts or Practices that Raise a Significant Risk of Concrete Harm Violate Section 5

The Commission should reject Respondent's argument that a "significant risk of concrete harm" fails to establish substantial injury under Section 5(n). Respondent argues that a "plain reading" of Section 5(n) reveals that the statute does not use the words "significant risk of concrete harm" and that Congress "would have included such language in the statute" if it intended "significant risk of concrete harm" to be the standard of proof. RAB 17-19, 34-35.

[6] While *American Financial* case was decided before Congress codified the Unfairness Statement, the court analyzed the Commission's actions under the factors later codified as Section 5(n).

Respondent further argues – citing nothing other than the Initial Decision – that Congress "considered but rejected" the "significant risk of concrete harm" standard contained in the Unfairness Statement when it enacted Section 5(n). RAB at 34-35 (quoting ID at 54-55).

The term "substantial injury" includes "significant risk of concrete harm," as demonstrated by the legislative history and caselaw discussed in Complaint Counsel's opening brief. CCAB at 11-17. Section 5(n) does not define the term "substantial injury," a term of art that Congress drew directly from the Commission's Unfairness Statement. Where a statutory term is capable of different meanings, it is appropriate to review the legislative history. *See, e.g.*, *Campaign for a Prosperous Ga. v. SEC*, 149 F.3d 1282, 1286 (11th Cir. 1998) ("An ambiguous statutory phrase should be construed in the context in which it is used, with the congressional intent in mind.") (citing *Robinson v. Shell Oil Co*., 519 U.S. 337 (1997)).[7] Here, the legislative history leaves no doubt that Congress specifically intended to adopt the principles of the Commission's Unfairness Statement in full. *See* CCAB at 13-14; H.R. Conf. Rep. No. 103-617, 1994 WL 385368, at *11-12 (1994); S. Rep. No. 103-130, 1993 WL 322671, at *12 (1993) ("This section is intended to codify . . . the principles of the FTC's December 17, 1980, policy statement on unfairness . . . . Since the FTC's policy statement itself is based on the FTC's decided cases and rules, this section codifies existing law."); *FTC v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 937 n.5 (N.D. Ill. 2008) ("The legislative history demonstrates that Congress's

[7] There is no conflict between the language of the statute and its interpretation. Rather, the legislative history explains what Congress intended the phrase "substantial injury" to mean. However, even where the plain meaning of a statutory term is directly contradicted by "a clearly expressed legislative intention," the cases Respondent cites recognize that the plain meaning is not conclusive. *CPSC v. GTE Sylvania, Inc.*, 447 U.S. 102, 108 (1980); *see also Consol. Bank, N.A. v. U.S. Dep't of Treas.*, 118 F.3d 1461, 1463 (11th Cir. 1997) ("We are required to look beyond the plain language of the statute . . . when Congress clearly has expressed an intent contrary to that suggested by the plain language . . . ."); *Gonzalez v. McNary*, 980 F.2d 1418, 1420 (11th Cir. 1993) (ordinary language is dispositive "absent a clearly expressed legislative intent to the contrary"); *Hudgins v. City of Ashburn*, 890 F.2d 396, 405 (11th Cir. 1989) (same); *Blue Cross & Blue Shield of Ala. v. Weitz*, 913 F.2d 1544, 1548 (11th Cir. 1990) (same).

intent was to codify the FTC's Unfairness Policy Statement of 1980 . . . ."). *Cf. also Merck & Co., Inc. v. Reynolds*, 559 U.S. 633, 648 (2010) ("We normally assume that, when Congress enacts statutes, it is aware of relevant judicial precedent."). Because the Unfairness Statement explains that an injury is "sufficiently substantial . . . if it raises a significant risk of concrete harm," and the clear legislative intent was to codify the Unfairness Statement, the term "substantial injury" within Section 5(n) includes "significant risk of concrete harm."

Respondent also argues that a "significant risk of concrete harm" cannot be "substantial injury," because "Section 5(n) and apposite case law require that substantial injury must be likely to occur under the facts of this case." RAB at 35. Likewise, amicus TechFreedom argues that Complaint Counsel's interpretation of "significant risk of concrete harm" as "substantial injury" would read the word "likely" out of the statute. TFA at 6, 12 n.8. To the contrary, Section 5 sets out two alternative justifications for Commission action – where a practice currently causes a significant risk of concrete harm, or where a practice is likely to do so in the future. The statute distinguishes the temporal nature of the substantial injury that each alternative is intended to address by use of verb tense: "causes . . . substantial injury" for practices that currently cause a significant risk of concrete harm and "is likely to cause substantial injury" for those that are likely to cause such injury in the future.

Finally, Respondent contends that, in prior cases, Section 5 unfairness liability has been found only where "actual harm" has occurred. RAB at 36.[8] Respondent ignores the Commission's decision in *this* case, where the Commission concluded that data security practices may violate Section 5(n) even where no breach has occurred. Comm'n Order Denying Mot. to Dismiss at 19.[9] In any event, that earlier unfairness cases alleged economic and other completed harms does not change the meaning of the statute. *See Wyndham*, 799 F.3d at 246 ("[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs.").

---

[8] Respondent ignores a recent case in which the federal district court judge granted the Commission's TRO application after a debt collection company, similar to the 1718 File incident, placed consumer personal information on the public Internet. *FTC v. Cornerstone & Co., LLC*, No. 1:14-CV-01479, Section IV at 7 (Prelim. Injunct.) (D.D.C. Sept. 10, 2014), https://www.ftc.gov/system/files/documents/cases/141001cornerstoneorder.pdf. Similar to the allegations in this case, the Commission argued that "Defendants' unlawful conduct has caused substantial harm and injury to consumers' privacy and is likely to cause substantial additional harm, such as identity theft, including existing and new account fraud, and other consumer injury." *FTC v. Cornerstone & Co., LLC*, No. 1:14-CV-01479, Memorandum In Support of Plaintiff's Application for Temporary Restraining Order at 10-11 (Aug. 27, 2014), https://www.ftc.gov/system/files/documents/cases/141001cornerstonetro.pdf. The Commission did not allege that identity theft had already been known to have occurred.

[9] The ID failed to follow the law of the case established by the Commission in its order denying LabMD's motion to dismiss. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 18 (ruling that complaint allegations that data security practices caused (1) actual data breaches, enabling unauthorized persons to obtain sensitive consumer information, as well as (2) increased risk of other potential breaches were sufficient, if proven, to establish that Respondent's data security procedures caused, or were likely, to cause consumer harm). Under the law of the case doctrine "an appellate decision is binding in all subsequent proceedings in the same case." *Litman v. Mass. Mut. Life Ins. Co.*, 825 F.2d 1506, 1510 (11th Cir. 1987). The ID cited no exceptions to the law of the case doctrine that would justify departing from it: there has been no "intervening change in the controlling law," nor is the Commission's reasoning "clearly erroneous" such that it would create a "manifest injustice" if implemented. *Id.* at 1510-11 (also noting that law of the case may be inapplicable if prior decision spoke to a specific set of facts and there had been a change in evidence).

For the same reasons, the Commission should decline to reconsider its decision on the Motion to Dismiss. To do otherwise would invite parties to continuously re-litigate issues and eliminate the efficiency and finality in Commission decisions. *Litman*, 825 F.2d at 1510; *see also Alphamed, Inc. v. B. Braun Med., Inc.*, 367 F.3d 1280, 1285-86 (11th Cir. 2004) (noting that courts are generally bound by a prior decision in the same case because otherwise "there would be no end to a suit [because] every obstinate litigant could, by repeated appeals, compel a court to listen to criticisms on their opinions or speculate of chances from changes in its members.") (internal quotations and citations omitted).

The Commission should reaffirm that a practice causes or likely causes substantial injury under Section 5(n) of the FTC Act if it "raises a significant risk of concrete harm." Comm'n Order Denying Resp't's Mot. to Dismiss at 19; *see also FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010) ("An act or practice can cause substantial injury by doing a small harm to a large number of people, or if it raises a significant risk of concrete harm."); CCAB at 11-12.

### C. Complaint Counsel Met Its Burden Under Section 5(n)

Respondent contends that Complaint Counsel has shown only that consumer injury is "possible," but not that injury is "probable" or "likely." RAB at 26, 33-34, 36, 43 n.17, 44. It argues that "[t]he 'possibility' of some unknown future 'risk' of concrete harm cannot satisfy the FTC burden of proof under Section 5(n)." RAB at 36. This argument not only ignores Complaint Counsel's expert testimony regarding the concrete harms that result from the types of multiple, systemic, and serious data security failures that LabMD engaged in, CCAB at 35-39, it is also unpersuasive as a matter of law.

Respondent first argues that Complaint Counsel must show that injury is "likely," which it defines as "probable." Respondent analogizes to the Commission's standard of deception, interpreting the phrase "likely to mislead" as requiring proof that deception was "probable" and not "possible." RAB at 36. It also cites to *In re Terazosin Hydrochloride Antitrust Litig.*, 352 F. Supp. 2d 1279 (S.D. Fla. 2005), for the proposition that the terms "likelihood" and "probability" are synonymous. RAB at 43-44. However, neither the Commission's deception standard nor the caselaw on preliminary injunctions cited in *Terazosin* is relevant to Section 5(n), which solely addresses unfairness. *See Yates v. U.S.*, 135 S. Ct. 1074, 1082 (2015) ("[I]dentical language may convey varying content when used in different statutes, sometimes even in different provisions of

the same statute.").[10] Moreover, as noted above, Complaint Counsel is not arguing that future LabMD practices are *likely* to cause substantial injury; rather, it is arguing that LabMD's practices created a significant risk of concrete harm and thus *caused* substantial injury. In any event, even assuming the test were whether LabMD's conduct was "likely" to cause injury, Complaint Counsel has more than met that test. *See generally infra* § V, at 19.

Of course, this does not mean that the "significant risk of concrete harm" standard is boundless, contrary to Respondent's argument. Respondent relies heavily on the Initial Decision's argument that "proof of risk of injury" would "effectively expand liability to cases involving generalized or theoretical 'risks' of future injury." RAB at 41-42 (quoting ID at 86). Trivial, speculative, or certain subjective harms, such as those that offend the tastes or social beliefs of particular consumers, do not meet the first prong of Section 5(n). Unfairness Statement, 1984 FTC LEXIS 2, at *307. In contrast, where, as here, the significant monetary and non-monetary risks associated with identity theft and medical identity theft have been well

[10] Even assuming the deception standard is relevant, the Policy Statement on Deception affirms that a practice is likely to mislead reasonable consumers if a "significant minority" of consumers are deceived. FTC Policy Statement on Deception at 10 n.20 (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf. The Commission and courts have held that a misleading interpretation shared by as few as 10% of consumers constitutes deception. *Telebrands, Inc.*, Docket No. 9313, 140 F.T.C. 278, 2005 WL 6241018, at *325 (2005) ("[T]he ALJ held correctly that as a matter of law the net takeaway – which ranged from 10.5% to 17.3% . . . – was sufficient to conclude that the challenged claims were communicated."); *see also Firestone Tire & Rubber Co. v. FTC*, 481 F.2d 246, 249 (6th Cir. 1973) (10%-15%); *Mut. of Omaha Ins. Co. v. Novak*, 836 F.2d 397, 400 (8th Cir. 1987) (10% in Lanham Act case); *Goya Foods, Inc. v. Condal Distribs., Inc.*, 732 F. Supp. 453, 456-57 (S.D.N.Y. 1990) (9%). Thus, the caselaw on deception supports a conclusion *contrary* to Respondent's argument that "likely" means "probable."

documented, a failure to protect the information used to commit such crimes unquestionably causes or is likely to cause substantial injury.[11]

As described in detail in Complaint Counsel's opening brief, LabMD's multiple, systemic, and serious data security failures left many gaping holes in its network, creating a significant risk of unauthorized disclosure of consumers' sensitive information to identity thieves and others. *See* CCAB 23-31. Section 5 liability under these circumstances does not depend on the happenstance of whether a company is breached and whether a victimized consumer can trace an identity theft incident back to the breached company.

### D. Section 5(n)'s Substantial Injury Standard is Broader than Article III's Standing Standard

Respondent wrongly invokes principles of private plaintiff Article III standing to suggest that Complaint Counsel must prove "injury-in-fact," a "directly traceable" injury, and proximate cause. RAB at 25. This is fundamentally incorrect. The FTC is not a private plaintiff seeking damages, but a federal agency acting under the authority conferred by Congress to enforce Section 5. *See, e.g., FTC v. CyberSpy Software, LLC*, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009) (holding "Congress has conferred standing on the FTC" to pursue Section 5 claims). Section 5(n) does not require proof of injury-in-fact or acts that are "directly traceable" to particular consumer injuries. Rather, an act or practice that causes or likely causes substantial injury is sufficient. As noted previously, the Commission has already determined that a

[11] Other federal agencies also apply a significant risk of harm standard without sanctioning "generalized" or "theoretical" risks. While these cases do not apply the FTC Act, they are instructive in analyzing significant risk. *See, e.g., Indus. Union Dep't v. Am. Petroleum Inst.*, 448 U.S. 607, 655-656 (1980) (the "*Benzene*" Cases) (in applying the Occupational Safety and Health Act, the Supreme Court recognized that a finding of "significant risk" must be supported by substantial evidence, but "need not be a mathematical straitjacket" nor be supported "with anything approaching scientific certainty"); *Ethyl Corp. v. EPA*, 541 F.2d 1, 18-20 (D.C. Cir. 1976) (upholding EPA conclusion that automotive emissions caused by leaded gasoline presented a "significant risk of harm," which was less than "probable" and "considerably more certain" than a "somewhat remote" risk).

significant risk of concrete harm constitutes substantial injury. *See supra* § IV.B at 8; CCAB at 21-22.

For this same reason, the Commission should reject Respondent's argument that there has been "no injury" in "data breach cases where no misuse is alleged[.]" RAB at 35 (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3rd Cir. 2011)). In *Reilly*, the court dismissed a private litigant's claim for damages on Article III standing grounds for a failure to establish injury-in-fact. 664 F.3d at 45. As noted above, Section 5(n) does not require such proof. In fact, the Commission approved a consent agreement with Ceridian Corporation and issued an order arising from the exact same data breach at issue in *Reilly*. *See Ceridian Corp.*, FTC File No. 102-3160 (2011).

Similarly, the Commission should reject Respondent's argument that Complaint Counsel must prove "proximate causation" and injury to a "victimized consumer." RAB at 25-26. Complaint Counsel has offered competent and reliable evidence that LabMD's multiple, systemic, and serious failures of data security caused, or likely caused, substantial injury to consumers as required under Section 5(n). Complaint Counsel need not establish that LabMD's failures caused specific harm to individual consumers, *see* CCAB 17-19, and the FTC Act does not require the Commission to wait for consumer injury before bringing an action. *See* Comm'n Order Denying Resp't's Mot. to Dismiss at 19; *Am. Fin. Servs. Ass'n*, 767 F.2d at 972; CCAB at 22.

### E. Section 5(n) Does Not Impose Strict Liability for Data Breaches

Respondent argues repeatedly that a finding that LabMD violated Section 5(n) would result in *per se* or strict liability for data breaches. *See, e.g.*, RAB at 23-24, 62, 63. This is plainly wrong. First, Respondent assumes that this case is only about the disclosure of the 1718

File; to the contrary, it is about the significant risk of concrete harm caused by LabMD's multiple, systemic, and serious data security failures. Second, as the Commission has stated in this case, a company that has maintained reasonable security would not be liable under Section 5 merely because a breach occurred. Comm'n Order Denying Resp't's Mot. to Dismiss at 18. Indeed, Respondent's strict liability argument ignores the three-prong unfairness analysis, focusing only on the injury prong, and only as that analysis relates to it making the 1718 File available on a P2P network.[12] While disclosure of certain sensitive information, including medical information, may cause injury to consumers, such disclosure does not *per se* violate Section 5; it only violates Section 5 if the company's practices that led to the disclosure were not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition.[13]

The relevant inquiry is the elements of Section 5(n), which Complaint Counsel has established. Complaint Counsel has proven that LabMD's data security failures, CCAB at 24-30, caused or were likely to cause substantial injury to consumers.[14] The exposure of consumer

---

[12] Even within the injury prong, as explained *infra* in Section V.A at 19, the failures that resulted in the 1718 File's exposure are not a complete picture of LabMD's unfair data security practices.

[13] Respondent makes much of footnote 9 on page 24 of Complaint Counsel's appellate brief. *See* RAB at 23, 26, 32, 33, 42, 62. Far from advocating for strict liability, footnote 9 stands for the unremarkable proposition that "unreasonable" data security practices are those that cause or are likely to cause substantial injury, that are not outweighed by the countervailing benefits to consumers or to competition, and are not reasonably avoidable by consumers.

[14] Respondent argues that "[t]he FTC characterization of the LabMD data security is irrelevant to the FTC burden of proof under Section 5(n), namely, that CC prove that the LabMD data security practices caused actual harm or are likely to cause substantial harm." RAB at 65. Here, Respondent itself seems to argue for a strict liability standard based only on harm, without regard to a company's conduct. This is contrary to Complaint Counsel's position, which regards LabMD's data security to be directly relevant. The Commission challenges "unreasonable data security measures (or other practices that enable[] unauthorized third parties to harm consumers by obtaining access to their confidential personal data) as 'unfair acts or practices' in violation of Section 5." Comm'n Order Denying Resp't's Mot. to Dismiss at 9. Harm in the absence of unlawful practices, including data security failures, does not violate Section 5.

information in the 1718 File increased that already-significant risk of concrete harm. CCAB at 8, 30-35. As explained further below, LabMD's actions also caused harm to consumers, because they experienced the loss of privacy of their sensitive personal and health information through the exposure of the 1718 File. *See infra* § IV.F at 17; CCAB at 9, 39-41. Consumers could not reasonably avoid this injury, CCFF ¶¶ 1773-1795, and the harm was not outweighed by countervailing benefits to consumers or competition, CCFF ¶¶ 1113-1185, 1798.

Section 5(n) in general and as applied in this case is a far cry from a strict liability statute. An enumeration of the evidence shows that Complaint Counsel does not argue that exposure of the 1718 File alone constitutes unfair conduct under Section 5. To the contrary, LabMD's liability arises from its multiple, systemic, and serious data security failures – some of which led to that exposure, and some of which resulted in other risks of concrete harm.

### F. Disclosure of Personal Information to Unauthorized Persons Injures Consumers

Disclosure of certain sensitive personal information, such as health information, injures consumers. Congress made this judgment in enacting HIPAA, state legislatures have made this judgment with respect to HIV testing and status,[15] and courts have made similar judgments. *See* CCAB 40-41; *see also Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 496 (Ga. Ct. App. 1994) (upholding, in invasion of privacy action, judgment against television station for revealing in public broadcast identity of person living with AIDS). In a situation analogous to the 1718 File incident, in which plaintiffs' medical records were available on the public Internet, a court declined to dismiss the case under Massachusetts privacy, tort, and contract law. *Walker v.*

[15] *See, e.g.*, Ga. Code Ann. §§ 31-22-9.1(a)(2)(D), 24-12-21(b)(1); Fla. Stat. § 381.004(2)(e), (f); Ala. Code § 22-11A-54.

*Boston Med. Ctr. Corp.*, No. 2015-1733-BLS-1, at 1 (Mass. Super. Ct. Nov. 19, 2015), Attachment 1. The court found that "plaintiffs' medical records were available to the public on the internet for some period of time and that there is a serious risk of disclosure. It is reasonable to infer the next step – that plaintiffs' records either were accessed or likely to be accessed by an unauthorized person." *Id.* at 2. Such "unwanted privacy intrusions," Comm'n Order Denying Resp't's Mot. to Dismiss at 1, injure consumers who suffer the loss of their privacy, regardless of the persons to whom the information is made available. *See* RAB at 36; *see, e.g.*, *FTC v. Accusearch, Inc.*, 2007 WL 4356786, at *8 (D. Wyo. Sept. 28, 2007) (finding that loss of privacy can result in a constellation of emotional harms that are "substantial and real and cannot fairly be classified as either trivial or speculative"); *cf. Walker*, No. 2015-1733-BLS-1, Attachment 1, at 2 ("[A] claim for invasion of privacy involving disclosure of confidential medical records may give rise to damages for mental distress, harm to interest in privacy and special or economic harm.").

The cases to which Respondent cites for its claim that consumers are harmed only by known identity theft, RAB at 66, are inapposite. The plaintiffs in each of them alleged they had suffered identity theft, and the courts expressly declined to consider whether other harms alleged in the complaints, such as increased risk of future identity theft, were sufficient to confer standing on the plaintiffs.[16] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1323 n.1 (11th Cir. 2012) (observing that while "[s]ome of our sister Circuits have found that even the threat of future identity theft is sufficient to confer standing in similar circumstances, . . . [p]laintiffs have alleged only actual – not speculative – identity theft"); *Smith v. Triad of Ala., LLC*, 2015 U.S. Dist.

---

[16] The law relating to the injury required for Article III standing does not apply to the Commission's actions under Section 5 of the FTC Act. *See supra* § IV.D at 14.

LEXIS 132514, at *26 (M.D. Ala. Sept. 2, 2015) (holding that "because Plaintiffs have alleged actual identity theft and an economic injury," the court did not need to determine whether standing would lie for plaintiffs' claims regarding a heightened risk of future identity theft), Mag. R&R adopted by 2015 U.S. Dist. LEXIS 130935 (M.D. Ala. Sept. 29, 2015).

## V. COMPLAINT COUNSEL PROVED THAT LABMD'S DATA SECURITY FAILURES CAUSED OR WERE LIKELY TO CAUSE SUBSTANTIAL INJURY

### A. LabMD's Data Security Failures from January 1, 2005, through the Time of Trial Raised a Significant Risk of Concrete Harm to Consumers

Respondent engages in misdirection by suggesting that Complaint Counsel's proofs regarding LabMD's unlawful data security practices were circumscribed to a narrow time period. RAB at 1, 14 n.4, 19-20, 33, 46 n.21 (citing CCAB at 4, 8). Rather, LabMD created a significant risk of concrete harm to consumers through its data security failures from at least January 1, 2005, through the time of trial. CCCL ¶ 117.[17] This significant risk was further magnified when LabMD's billing manager downloaded the LimeWire file-sharing software onto her work computer in 2005, designated nearly every file for sharing on the Gnutella P2P network, and made the 1718 File available on a P2P network for nearly a year, between June 2007 and May 2008. CX0008-0011, CX0697 (1718 File) (dated June 5, 2007); CCFF ¶¶ 1363-1372, 1395.

Respondent also erroneously asserts that Complaint Counsel alleges that LabMD's conduct created a significant risk of concrete harm "solely by the alleged LabMD sharing of patient files on the P2P Network." RAB at 57. However, Complaint Counsel's data security

[17] Dr. Hill determined that she did not have adequate information relating to LabMD's post-July 2010 security practices to provide an expert opinion on LabMD's security after that date; she drew no conclusion that its conduct was reasonable after July 2010. CX0740 (Hill Report) ¶¶ 4, 48. Complaint Counsel submitted evidence demonstrating that LabMD's unfair security failures continued after July 2010. CCRRFF ¶¶ 10a-11.

expert, Dr. Hill, described the myriad ways in which LabMD's data security failures created a significant risk of concrete harm. While many of these failures contributed to the exposure of the 1718 File on a P2P network, the significant risk of concrete harm was not limited to that exposure. For example, Dr. Hill described the ways that LabMD failed to protect against hacking and insider threats other than P2P sharing. *See, e.g.*, CX0740 (Hill Report) ¶¶ 68-69 (enumerating ways in which LabMD failed to assess risks against malicious intrusion), 84 (LabMD did not use adequate measures to prevent employees from accessing personal information not needed to do their jobs), 91 (LabMD failed to train IT personnel on evolving threats and how to protect against them), 95 (LabMD did not employ or enforce strong password policies), 100 (LabMD did not update software and operating systems to protect against hackers).

Respondent's focus on the disclosure of the 1718 File, rather than LabMD's conduct, fundamentally misapprehends Section 5's prohibition of unfair commercial practices, as well as the nature of Complaint Counsel's overwhelming evidence of LabMD's unfair security practices. In fact, as the Commission has stated, a breach is neither a necessary nor a sufficient condition for finding a Section 5 violation. Comm'n Order Denying Resp't's Mot. to Dismiss at 19. The time period for examining LabMD's unfair security practices is not limited to the yearlong window in which it made available the personal information of approximately 9,300 consumers on a P2P network, but rather the entire period since 2005 for which Complaint Counsel presented evidence of the company's data security practices.

### B. Complaint Counsel's Experts Provided Competent and Reliable Testimony

Complaint Counsel offered the opinions of four experts in this case, Dr. Raquel Hill, Mr. Rick Kam, Mr. James Van Dyke, and Dr. Clay Shields. Despite Respondent's repeated challenges, the ALJ denied motions *in limine* to exclude Complaint Counsel's experts, and the

Initial Decision made no finding that the experts are not qualified or not credible. CCAB at 36. Each of Complaint Counsel's experts provided opinions based on reliable methodology applied to the facts of this case that will assist the Commission in deciding key disputed issues.

In its brief, Respondent incorrectly urges the Commission to apply legal standards to expert opinions that are not supported by the Part 3 Rules of Practice, 16 C.F.R. § 3.31A, Federal Rule of Evidence 702, or Section 5(n). RAB at 43-44. Specifically, Respondent argues that: (1) expert opinion is required to prove unfairness under Section 5(n); and (2) this mandatory expert opinion must be "within a reasonable degree of certainty or probability."[18]

Respondent's arguments that expert opinion is required to prove unfairness under Section 5(n) and must satisfy "a reasonable degree of certainty or probability" – raised for the first time on appeal – are based on cases in which the Georgia Supreme Court decided issues of Georgia tort law. RAB at 43-44 (citing *Zwiren v. Thompson*, 578 S.E. 2d 862, 865-68 (Ga. 2003); *Blakely v. Johnson*, 140 S.E. 2d 857, 859 (Ga. 1965)). Georgia tort law does not dictate Complaint Counsel's evidentiary burden in this proceeding. *See, e.g.*, 15 U.S.C. § 45(a), 16 C.F.R. § 3.31A. Indeed, to prove negligence under Georgia tort law, a plaintiff must show that he or she suffered actual injury, and the *Zwiren* court simply held that expert testimony must show "proximate causation in terms stronger than that of medical possibility, *i.e.*, reasonable medical probability or reasonable medical certainty." 578 S.E.2d at 867. This is different from the Section 5 liability standard, which requires proof only that an act or practice caused or was likely to cause substantial injury. Regardless, a private tort action cannot be compared to a public enforcement action of a remedial statute. As noted above, the FTC is not a private

[18] In addition, Respondent suggests that Complaint Counsel's expert proofs must meet a "likelihood" or "probability" standard. *See supra* § IV.C, at 12-13 (discussing *Terazosin*).

plaintiff seeking damages, but a federal agency acting under the authority conferred by Congress to enforce Section 5. *See FTC v. CyberSpy Software, LLC*, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009); *Ayers v. Wolfinbarger*, 491 F.2d 8, 16 (5th Cir. 1974) ("We must be guided by the 'familiar canon of statutory construction that remedial legislation should be construed broadly to effectuate its purposes.'") citing *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967)). Finally, even if Section 5(n) requires an expert to satisfy a "reasonable degree of certainty or probability," Complaint Counsel has met that burden in this case, as explained below.

Further, Respondent renews its unsuccessful *Daubert* objections, and sets up straw-man challenges to many expert opinions on which Complaint Counsel is not relying. RAB at 45-46, 51-53, 55-57; *see infra* § VI.A at 32. Each of Complaint Counsel's experts is qualified in a relevant field under *Daubert* and Federal Rule of Evidence 702, and provided competent and reliable testimony. Moreover, as noted in *Daniel Chapter One*, the court's role as a "gatekeeper" pursuant to *Daubert* to prevent expert testimony from unduly confusing or misleading a jury has little application in a bench trial. Docket No. 9329, 2009 FTC LEXIS 85, at *21-22 (Apr. 20, 2009); *accord McWane, Inc.*, Docket No. 9351, 2012 FTC LEXIS 142, at *8-9 (Aug. 16, 2012); Order Denying Mots. *In Lim.* to Exclude Proffered Experts at 2 (May 5, 2014). Respondent has failed to show any reason to depart from this approach on appeal.

### 1. Dr. Hill Provided Competent and Reliable Testimony

Relying on her twenty-five years of experience in computer security, data privacy, and networking systems, Complaint Counsel's expert, Dr. Raquel Hill, opined that LabMD had multiple, serious, and systemic security vulnerabilities that could have been easily corrected at little or no cost. *See* CCFF ¶¶ 382-1187; CCAB at 26-30. Most importantly, Dr. Hill demonstrated that these vulnerabilities increased the risk of network compromise and the

unauthorized disclosure of vast amounts of sensitive personal information collected and maintained by LabMD.[19] CX0740 (Hill Report) at ¶¶ 17, 27, 49, 51-107; CCAB at 26-30.

While Respondent challenges Dr. Hill's ultimate conclusion that its data security practices were unreasonable, it does not dispute Dr. Hill's opinions, nor the underlying facts: (1) LabMD's computer network had multiple, systemic, and serious data security vulnerabilities; (2) these vulnerabilities could have been cured at little to no cost; or (3) these vulnerabilities increased the risk of network compromise and unauthorized disclosure. *See* RAB at 48-50 (discussing Dr. Hill's expert testimony in detail without challenging these findings).

Unable to contradict Dr. Hill's key findings, Respondent instead argues that Dr. Hill's opinions should not apply to LabMD – first because they relate only to general computer security practices and not to the healthcare industry in particular; and second, because they are valid only for computer security practices after 2009. As discussed *supra* in Section III.B at 6, Dr. Hill explained that the guidelines for protecting computer infrastructure are common across all industries:

> Computing is pervasive, so these guidelines, whether they're from NIST or from the Computer Emergency Response Team or from the National Research Council that specifically focused on medical data, they have consistent guidelines. And that's because computing is pervasive and consistent across different types of business domains.

Hill, Tr. 234-35; *see also* Hill, Tr. 295-96; RX524 (Hill, Dep. at 61-62); CCRRFF ¶¶ 318, 363. Dr. Hill described the security standards set forth in her expert report as identifying the "basic requirements" for securing any system that collects and stores consumers' sensitive personal information:

[19] While Dr. Hill testified that each specific security vulnerability increased the risk of network compromise and unauthorized disclosure, the ALJ wrongfully excluded her opinion that LabMD's overall data security practices increased the risk of unauthorized disclosure and network compromise. *See* CCAB at 25, n.10.

> The recommendations that I laid out in my expert witness document contain basic requirements for securing a system. These are consistent with recommendations by governmental and industry and academic institutions working together to define and specify such recommendations. So it is expected that an organization will apply updates to their software. It is expected that they will have strong passwords. It would – it is expected that they would implement access control mechanisms. It is expected that they would assess their networks for emerging vulnerabilities. So what I've recommended is what these other guidelines recommend. These are the basic things that you must do to have reasonable and appropriate security for your system.

Hill, Tr. 295-96; *see also* CCRRFF ¶¶ 318, 344, 363.

The basic requirements described by Dr. Hill were widely known and used during the time period for which Dr. Hill had sufficient information to render an expert opinion of LabMD's data security practices. The underlying principles described in Dr. Hill's report for implementing a layered data security strategy[20] to protect computer networks were widely available from many sources.[21] For example, in 2002, the National Institute for Standards and Technology ("NIST") published a standard setting forth a nine-step layered data-security process. CCFF ¶¶ 491-492. Under guidance available at the time, LabMD knew or should have known to implement a layered defense strategy to protect its computer networks. *See* CCRRFF ¶¶ 318, 340.

---

[20] While Dr. Hill testified that she may not have used the exact term "Defense-in-Depth" throughout the time period to which her report relates, a fact of which Respondent makes much, RAB at 16, Dr. Hill's opinion was clear that terminology aside, a company must implement a layered defense approach to protect sensitive information on its network. CX0740 (Hill Report) ¶¶ 27 ("In such an approach, the network is viewed as a system with multiple layers, and security mechanisms are deployed at each layer to reduce the overall likelihood that an attack will succeed."), 51-106 (setting forth LabMD's multiple security failures).

[21] The FTC's 24-page "Protecting Personal Information" business guide, first published in 2007, CCRRFF ¶¶ 90, 340, rather than 2011 as Respondent claims, RAB at 47 n.22, also describes a layered security concept. *See* CCRRPTB at 12-15 (describing in detail how FTC business guidance was consistent with security principles in Dr. Hill's expert report). Another source of guidance is the System Administration, Networking, and Security Institute ("SANS") security training and materials for practitioners who maintain and operate computer systems, and vulnerability information from the Global Information Assurance Certification organization ("GIAC"). CCFF ¶¶ 494-495.

Finally, Respondent argues that only Dr. Hill could have opined that LabMD's data security practices were likely to cause substantial consumer harm, but that she did not do so. RAB at 48-50. Complaint Counsel, however, is not required to present its case through only one expert witness. Rather, Dr. Hill, the experienced data security expert, opined on how LabMD's data security practices increased the risk of network compromise and unauthorized disclosure of vast amounts of sensitive personal information for hundreds of thousands of consumers. As explained further *infra*, Complaint Counsel's other experts, Mr. Kam and Mr. Van Dyke, testified as to the concrete harms caused by such exposure of sensitive personal information, including identity theft and medical identity theft. *See* CCFF¶¶ 1472-1766*; see also infra* § V.B.2-3 at 25-30.

### 2. Mr. Kam Provided Competent and Reliable Testimony

Mr. Kam provided competent and reliable expert opinion on which the Commission should rely. As an initial matter, Complaint Counsel is not relying in this appeal, nor did it rely below, on any opinions predicated on Mr. Boback's testimony (CX0703; RX541) or a document produced by Tiversa purporting to show "spread" of the 1718 File (CX0019). Complaint Counsel is not relying upon many of Mr. Kam's opinions that Respondent challenges. RAB at 51-54. For example, Complaint Counsel did not cite Mr. Kam's injury calculations for medical identity theft for consumers in the 1718 File, CX0742 (Kam Report) at 19-21, because the calculations were based on Mr. Boback's testimony that the 1718 File had been found on a P2P network in 2013. *See infra* § VI.A at 32.

Respondent challenges Mr. Kam's expertise, but its position is directly contravened by the facts of this case. RAB at 51. Mr. Kam, a Certified Information Privacy Professional, leads and participates in several cross-industry data privacy groups, regularly publishes relevant

articles in the field, and works on development of policy and solutions to address the protection of health information and personally identifiable information ("PII"), as well as remediating privacy incidents, identity theft, and medical identity theft. CCFF ¶ 38. Mr. Kam is president and co-founder of ID Experts, a company specializing in data breach response and identity theft restoration. CCFF ¶ 38. Based on a thorough literature review, documents Mr. Kam received from Complaint Counsel, and his professional experience and qualifications, Mr. Kam offered opinions assessing the risk of injury to consumers caused by the unauthorized disclosure of consumers' sensitive personal information. CCFF ¶¶ 39-41.

Respondent asserts that Mr. Kam's methodology is not "peer reviewed," published, or used by others in similar fields. RAB at 51. But there are several different means to assess the reliability of an expert's methodology in addition to the specific *Daubert* factors Respondent cites. *See Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 593-95 (1993) ("The inquiry envisioned by Rule 702 is, we emphasize, a flexible one."); *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 150-51 (1999) (*Daubert* factors are "meant to be helpful, not definitive"). Because there are many types of experts and many types of expertise, the relevant reliability concerns may focus upon the expert's personal knowledge or experience. *See Kumho*, 526 U.S. at 150; Fed. R. Evid. 702 advisory committee's note (2000 amendment) (expert may rely "solely or primarily on experience" where the expert has "explain[ed] how that experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts"); *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 691 F. Supp. 2d 448, 473-74 (S.D.N.Y. 2010) (applying advisory committee note's standard for experience qualifying an expert).

In this proceeding, Mr. Kam's analysis of the risk of consumer injury is a fact-dependent inquiry based on his extensive experience working in the field of identity theft victim restoration, as well as his knowledge of relevant literature concerning identity theft, medical identity theft, and consumer privacy. CX0742 (Kam Report) at 3-6, 10-11, 13-15, 33-36; RX522 (Kam, Dep.) at 36-37, 44-46, 72-73. In analyzing the harm of unauthorized disclosures, Mr. Kam considers the nature and extent of the sensitive personal information involved in an unauthorized disclosure, including the types of identifiers and the likelihood of re-identification; the unauthorized persons who used the protected health information or to whom the disclosure was made; whether the sensitive personal information was actually acquired or viewed; and the extent to which the risk to the protected health information has been mitigated. CX0742 (Kam Report) at 17-18; CCFF ¶ 43.

Mr. Kam derived this framework from his work with clients, which he outlined throughout the report, as well as his literature review. CX0742 (Kam Report) at 10, 13-15, 33-36; RX522 (Kam, Dep.) at 36-37, 44-46, 72-73. Mr. Kam's judgment in assessing how each unauthorized disclosure or security failure creates particular risks is informed by years of experience in responding to unauthorized disclosures. CX0742 (Kam Report) at 3, 13-15. Mr. Kam explains in detail how he applied his experience to the facts of the Sacramento Day Sheets and LabMD's security failures; how his experience led to his opinions on the likelihood of harm resulting from the disclosure of sensitive personal information held by LabMD; and why his experience provides sufficient bases for those opinions. CX0742 (Kam Report) at 10-12, 18-19, 21-23.

Although Complaint Counsel is not relying on Mr. Kam's specific calculations of harm based on the 1718 File, it is relying on his calculation of harm to individuals included in the

Sacramento Day Sheets[22] based on the 2013 Ponemon Survey. *See* CCFF ¶¶ 1507, 1602-03, 1621. Respondent cannot successfully challenge the survey methodology. It has not offered any competent evidence that diminishes the reliability or outcome of the survey based on the response rate, any alleged non-response bias, or sampling frame bias. CCRRFF ¶¶ 403, 405, 407.

Finally, the Commission should reject Respondent's suggestion that Mr. Kam's opinions are not reliable, because he assumed a fact established by other evidence – that LabMD failed to provide reasonable data security. RAB at 52. "[A]s a practical matter, experts may express opinions based upon hypotheticals and information which would otherwise be inadmissible hearsay on its own. Additionally, experts can rely upon the opinions of other experts." *MediaTek Inc. v. Freescale Semiconductor, Inc.*, 2014 WL 971765, at *1 (N.D. Cal. Mar. 5, 2014); *see also U.S. v. 1,014.16 Acres of Land, More or Less, Situated in Vernon Cty., State of Mo.*, 558 F. Supp. 1238, 1242 (W.D. Mo. 1983) *aff'd*, 739 F.2d 1371 (8th Cir. 1984).

### 3. Mr. Van Dyke Provided Competent and Reliable Testimony

Mr. Van Dyke presented competent and reliable expert opinion on which the Commission should rely. As with Mr. Kam, Complaint Counsel did not rely on opinions predicated on Mr. Boback's testimony (CX0703; RX541) or CX0019. Complaint Counsel is not relying upon many of Mr. Van Dyke's opinions that Respondent challenges in its answering brief. RAB at 54-57. For example, Complaint Counsel did not cite Mr. Van Dyke's injury calculations for consumers in the 1718 File, CX0741 (Van Dyke Report) at 12, because the calculations were

[22] Respondent's puzzling assertion that Complaint Counsel did not prove that the Sacramento documents were found in the hands of known identity thieves, RAB at 23 n.6, is patently wrong. *See* CX0090-CX0092, CX0107-CX0110 (substantiating that Day Sheets were found in possession of individuals who later pleaded no contest to identity theft).

based on Mr. Boback's testimony that the 1718 File had been found on a P2P network in 2013. *See infra* § VI.A at 32. The Commission should therefore disregard Respondent's challenges to Mr. Van Dyke's methodology regarding his calculations based on the purported spread of the 1718 File. RAB at 55-57.

Although Complaint Counsel is not relying on these calculations, Mr. Van Dyke's presentation of Javelin's 2010-13 Identity Fraud surveys illustrates that data breach victims experienced identity fraud at rates seven to eleven times that of consumers who had not been notified they were involved in a data breach, with absolute rates of 11.8% to 30.5%. CX0741 (Van Dyke Report) at 7, 8 Fig. 1.

Based on a thorough review of the facts of this case and his experience and professional qualifications, Mr. Van Dyke offered opinions assessing the types of concrete harms that occur when consumers' PII is not adequately protected from unauthorized disclosure. CCFF ¶¶ 24-25. Mr. Van Dyke testified at length regarding the methodology used in forming his opinions, demonstrating that it is reliable and will assist the trier of fact. CCFF ¶¶ 30-36; Van Dyke, Tr. 601-11, 617-32.[23]

Respondent argues that Mr. Van Dyke's analysis did not account for different types of data breaches by different actors, and contends these factors may be relevant to consumer injury. RAB at 55. As Mr. Van Dyke explained, based on survey data he has fielded for ten years and his considerable experience, the exact profile of a recipient of unauthorized information is not

[23] Respondent's assertion that Mr. Van Dyke did not consider the "specific facts of the case" is misleading. RAB at 55. Mr. Van Dyke explained that his "analysis is about the relationship between exposure of PII and the risk of harm, and the method by which that data was exposed or might have been exposed did not factor into that analysis." RX523 (Van Dyke, Dep.) at 41. Thus, Mr. Van Dyke's comprehensive survey examined whether consumers who received notice that their PII was compromised in a data breach were at an increased risk of identity fraud. In 2013, the survey found that nearly one in three such consumers reported becoming the victim of identity fraud in the past twelve months. CCFF ¶ 1507.

important for predicting in a statistically significant manner what is likely to occur next. Van Dyke, Tr. 734. The single overriding factor in calculating fraud impacts is whether the individual was authorized to receive the information. *Id.* Moreover, Mr. Van Dyke testified that he specifically considered whether the Sacramento Day Sheets were "in the hands of unauthorized parties" and he was aware those documents "were found in the possession of individuals that have pleaded no contest to identity theft." Van Dyke, Tr. 645-46; *see also* CCFF ¶¶ 1413-1458. Respondent has not addressed any of this testimony. Nor has Respondent shown that incorporating additional factors, such as the type of breach or profile of the unauthorized recipient, would have altered Mr. Van Dyke's analysis.

The Javelin Survey results are sufficiently connected to the facts of this case. *See* RAB at 20-21. The known exposure of sensitive personal information contained in LabMD's Day Sheets occurred in 2013. Regardless of the manner in which the identity thieves obtained the Day Sheets, this is "the most probative indirect evidence . . . available" of the fact that the information in LabMD's possession is the type that is valuable to identity thieves, and that identity thieves have incentives to obtain this information. *Int'l Harvester*, 1984 FTC LEXIS 2, at *253 n.52.

The Commission should also reject Respondent's claim that Mr. Van Dyke improperly assumed LabMD failed to provide reasonable data security. RAB at 54. As discussed above, *see supra* at 28, it is well-settled that an expert may properly rely on facts that are established by other evidence.

#### 4. Dr. Shields Provided Competent and Reliable Testimony

Respondent's claim that Dr. Shields failed to provide reliable evidence about the risk created by LabMD's inadequate security is based on a misreading of the record that ignores substantial portions of Dr. Shields's testimony and report. RAB at 57-58. Contrary to

Respondent's claim that "there is no opinion of the probability of likely substantial harm within his testimony," RAB at 58, Dr. Shields's report and testimony state that even if it were unlikely that any given user would locate the 1718 File, with millions of users on the P2P network at a given time it would be expected that the file would be found many times.[24] Shields, Tr. 873-74; CX0738 (Shields Rebuttal Report) ¶¶ 59-61. In addition, Dr. Shields discussed at length several ways that malicious users could locate the 1718 File with relative ease, even if they did not know the name of the file or its specific nature. Shields, Tr. 867-69, 872-73; CX0738 (Shields Rebuttal Report) ¶¶ 56-58, 64-76.

Respondent similarly misrepresents the record when it states that "Professor Shields has limited, if any, experience with LimeWire." RAB at 62. This ignores the undisputed fact that Dr. Shields has extensive experience with the Gnutella network, which provides the protocols that LimeWire uses, and P2P networks in general. Shields, Tr. 812, 814-15; CX0738 (Shields Rebuttal Report) ¶¶ 7, 9. Indeed, Dr. Shields was involved in the development of a modified Gnutella client that is used by law enforcement to investigate child pornography on the Gnutella network. Shields, Tr. 814-15; CX0738 (Shields Rebuttal Report) ¶ 9.

Respondent also misrepresents the evidence by stating that "Professor Shields' opinions were based on" Mr. Boback's testimony. *See* RAB at 62. While Mr. Boback's deposition was among the material reviewed by Dr. Shields in preparation for forming his opinion and writing his report, Dr. Shields did not base any of his opinion on any fact set forth in that deposition. *See*

[24] Respondent's counsel elicited testimony from Dr. Shields that finding any particular file on a P2P network is like winning the lottery. Shields, Tr. 917. Although finding the 1718 File through a single search may be like winning the lottery, with millions of users conducting searches over an extended period, Dr. Shields explained that some of them were bound to win the lottery. CX0738 (Shields Report) ¶¶ 60-61. When Dr. Shields offered, "And if you'd like, we can consider the odds," Respondent's counsel cut him off, stating "I don't want to consider the odds because I don't want to." Shields, Tr. 917.

Shields, Tr. 904-05 (stating that, while he did read Mr. Boback's deposition, he did not recall the details because it did not play a major role in his opinion). Respondent does not and cannot point to any portion of Dr. Shields's opinion that relied on Mr. Boback's testimony.

Instead of squarely addressing the actual contents of Dr. Shields's testimony and report, Respondent instead argues that Dr. Shields's testimony about the real and substantial risk created by allowing the 1718 File to be placed on the Gnutella network should be ignored, because there is no evidence that any particular user other than Mr. Wallace downloaded the 1718 File from the network. *See* RAB at 58. This ignores the fact that a practice can violate Section 5 by creating a significant risk of concrete harm. *See supra* § IV.B at 8. Dr. Shields testified extensively about the risk created by allowing the 1718 File to be shared on the Gnutella network. *See* Shields, Tr. 867-69, 872-73; CX0738 (Shields Rebuttal Report) ¶¶ 56-58, 64-76. Respondent also ignores the fact that the only computer from which definitive evidence regarding the downloading of the 1718 File by users other than Mr. Wallace could have been obtained was destroyed during a LabMD forensic examination before Complaint Counsel could examine it. CCFF ¶ 1409; Shields, Tr. 856-58, 863.

## VI. RESPONDENT'S BRIEF MISCHARACTERIZES THE FACTS AND THE LAW

### A. Complaint Counsel Did Not Rely on Evidence Provided By Mr. Boback or Tiversa

Contrary to Respondent's claim that Complaint Counsel "violated its representation to the Tribunal . . . that 'it would not rely on expert opinion based on the testimony of Mr. Boback or on CX0019,'" RAB at 53, the record is unambiguous that Complaint Counsel did not rely on any such evidence. This may explain Respondent's failure to provide any citations to Complaint

Counsel's briefing to show otherwise.[25] Respondent's claim, and the portion of the Initial Decision to which it cites for this claim, ID at 10-11, 61, fundamentally misreads the record and ignores numerous statements by Complaint Counsel that it did not rely on any testimony from Mr. Boback or on CX0019, a document that purports to show the "spread" of the 1718 File. *See* Compl. Counsel's Opp'n to Resp't's Mot. to Admit Select Exs. at 10-11 n.11 (June 24, 2015); *see also* Compl. Counsel's Resp. to Resp't's Mot. to Refer Tiversa and Boback for Criminal Investigation at 2 n.1 (July 1, 2015); CCPTB at 61 n.3; CCRRPTB at 11.

Complaint Counsel's experts prepared their reports long before Mr. Wallace testified in this matter, and based them partially on the deposition testimony of Mr. Boback. Specifically, in Mr. Boback's November 21, 2013, deposition, he testified that "several weeks ago, we also performed a search to find the 1718, document to find, if it was located anywhere else through the peer-to-peer networks" and that "we found this in multiple locations." CX0703 (Boback, Tiversa Designee, Dep.) at 9-10. Accordingly, some of Complaint Counsel's experts based discrete portions of their reports on the assumption that the 1718 File had been located on the P2P network as late as 2013.

On May 30, 2014, during trial and long after the expert reports had been completed and submitted to the Court, Mr. Boback's counsel informed Complaint Counsel that when Mr. Boback testified that Tiversa had searched for the 1718 File in November 2013, he meant that Tiversa had searched only on its internal systems and had not searched the P2P network. *See* Tr.

[25] Respondent quotes the Initial Decision, which in turn cites to instances in which Complaint Counsel cites to Mr. Boback. These citations are to Complaint Counsel's responsive pleadings, where Mr. Boback was cited for the purpose of responding to Respondent's ancillary factual assertions. *See, e.g.*, CCRRFF 72b-74b (observing that Mr. Wallace's testimony on Tiversa's business methods is contradicted by Mr. Boback's). Complaint Counsel has not and does not rely on this or any other evidence supplied by Mr. Boback in support of its case-in-chief.

1227-28 (referencing CX0703).[26] Complaint Counsel immediately brought this to the Court's attention to promptly fulfill its ethical obligations under Rule of Professional Conduct 3.3. The Court accepted Complaint Counsel's discharge of its ethical obligation. Tr. 1229-30.

Following Mr. Wallace's testimony on May 5, 2015, which contradicted Mr. Boback's testimony and CX0019, Complaint Counsel determined it would not rely upon any portion of Mr. Boback's testimony or related evidence, including expert conclusions predicated on those sources. *See* Compl. Counsel's Opp'n to Resp't's Mot. to Admit Select Exs. at 10-11 n.11 (June 24, 2015). Accordingly, since Mr. Wallace's testimony, Complaint Counsel has not cited to or otherwise relied on Mr. Boback's testimony, CX0019, or any expert testimony that was based on this evidence in order to meet its burden of proof; its only citations to this evidence have been for the purpose of responding to Respondent's factual and legal assertions. *See*, *e.g.*, CCRRPTB at 71-73.

Respondent's assertion that Complaint Counsel has relied on expert opinions based on Mr. Boback's testimony and CX0019 is erroneous. Neither Dr. Hill nor Dr. Shields relied on Mr. Boback's testimony or CX0019 in reaching their opinions. The portions of Mr. Van Dyke's and Mr. Kam's reports and testimony relied upon by Complaint Counsel to meet its burden are independent of this evidence. *See supra* § V.B.2-3 at 25-30.

[26] In Mr. Boback's November 21, 2013, deposition, he testified that "several weeks ago, we also performed a search to find the 1718 document," and that "we found this in multiple locations." CX0703 (Boback, Tiversa Designee, Dep) at 9-10. Considerably later in his deposition, during testimony that did *not* relate to Tiversa's search of the P2P networks for the 1718 File, Mr. Boback noted the following: "We did not go and do any further investigation with Eagle Vision technology regarding this file or any other LabMD information, only internally did we search." *Id.* at 39.

### B. The Proceeding Against LabMD Does Not Violate the Fourth Amendment

Respondent repeatedly asserts that Complaint Counsel's reliance on the 1718 File – evidence it argues was obtained by Mr. Boback and Tiversa illegally or wrongfully – tainted this entire proceeding or violated the Fourth Amendment. RAB at 8, 37, 43 n.18, 63 n.25, 64; *see also* TFA at 16. This conclusory legal assertion of illegality is incorrect. LabMD exposed the 1718 File on a P2P network, and courts have recognized that such networks are public, as discussed below. Regardless, the Commission has already held that the exact mechanism of exposure of the 1718 File is not material to the Complaint's allegations. Comm'n Order Denying Resp't's Mot. for Summ. Decision at 6-7.

Actions of a private party, such as Tiversa, cannot violate the Fourth Amendment, even if the private party later gives evidence it obtained to the government. *See, e.g.*, *U.S. v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990) ("[W]here a private person delivers the fruits of his private search to police, that evidence is not excludable at trial on the basis that it was procured without a search warrant."); *U.S. v. Jacobsen*, 466 U.S. 109, 113-14 (1984) (Fourth Amendment is "wholly inapplicable" to searches by private parties); *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). The Supreme Court has clarified that the government "can be held responsible for a private decision *only* when it has exercised *coercive power* or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State." *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982) (citations omitted) (emphasis added). Here, the record contains no evidence whatsoever of such conduct by the Commission or its staff.

Further, because there is no evidence that Mr. Boback or Tiversa acted at the direction of or in conjunction with the Commission or its staff, the exclusionary rule is inapplicable here. "Misconduct by other actors is a proper target of the exclusionary rule only insofar as those

others are 'adjuncts to the law enforcement team.'" *U.S. v. Herring*, 492 F.3d 1212, 1217 (11th Cir. 2007) (quoting *Arizona v. Evans*, 514 U.S. 1, 15 (1995)). The Fourth Amendment protects an expectation of privacy against unreasonable government intrusion, not "the mere expectation . . . that certain facts will not come to the attention of the authorities." *Jacobsen*, 466 U.S. at 122.

The legal authority to which Respondent cites in support of its contention that Complaint Counsel may not rely on any evidence or fruits thereof that were wrongfully obtained is inapposite. RAB at 64. In *Knoll Associates, Inc. v. FTC*, unlike here, the private citizen's actions could be attributed to government encouragement or participation. 397 F.2d 530, 533-34 (7th Cir. 1968). Further, several Seventh Circuit opinions since *Knoll* have clarified that a finding of government complicity requires proof that: (1) the government knows of and acquiesces in the intrusive conduct (*i.e.*, that which invades another person's reasonable expectation of privacy); *and* (2) the private party's purpose was to assist law enforcement efforts (as opposed to furthering his or her own ends). *See, e.g.*, *U.S. v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987); *U.S. v. Harper*, 458 F.2d 891 (7th Cir. 1971); *U.S. v. Billingsley*, 440 F.2d 823, 826 (7th Cir. 1971). More than a year passed between when Tiversa first contacted LabMD and provided it with the 1718 File, and when the FTC sought a list of files Tiversa had discovered on P2P networks through compulsory process, which reinforces the Commission's lack of involvement.[27] *See, e.g.*, *NLRB v. South Bay Daily Breeze*, 415 F.2d 360, 363 (9th Cir. 1969) (finding *Knoll* inapplicable where "document was taken prior to the election and some time before the[] proceedings were initiated"). The facts fall squarely within the Supreme Court's holdings in *Jacobsen* and *Burdeau*.

[27] LabMD was one of nearly a hundred companies identified in response to the Commission's subpoena. Wallace, Tr. 1358, 1361-63.

Furthermore, to the extent that the Fourth Amendment has any applicability in this case – which it does not – numerous courts have held in a Fourth Amendment analysis that there is no reasonable expectation of privacy in files made available for sharing on a P2P network. *See, e.g.*, *U.S. v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011); *U.S. v. Stults*, 575 F.3d 834, 842-43 (8th Cir. 2009); *U.S. v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008). Here, it is undisputed that the 1718 File was available on a P2P network. CX0008-0011, CX0697; CCFF ¶¶ 1369, 1393.

### C. Respondent's Brief Cites to Evidence Properly Excluded by the ALJ

Respondent cites a staff report prepared for Representative Darrell Issa – a document that was not admitted below – to support its specious contention that the FTC knew that receiving documents from the Privacy Institute made it a party to conduct that allegedly violated HIPAA. RAB at 37, 64; *see also* TFA at 4.[28] Aside from being factually wrong, Respondent fails to acknowledge that the ALJ did not admit RX644 for the truth of the matters asserted therein, on the basis that those statements constitute unreliable hearsay.[29] Order on Resp't's Mot. to Admit Exs. at 3 (July 15, 2015). While any excluded evidence is retained in the record and available for any reviewing authority, *see* 16 C.F.R. §§ 3.43(i), 3.54(a) & (c), Respondent does not

---

[28] In their briefing, Respondent and its Amicus include a number of unsupported and inflammatory assertions regarding Complaint Counsel's conduct. *See, e.g.*, RAB at 53, 64; TFA at 4. Complaint Counsel's instant brief addresses only those allegations that are germane to the legal and factual issues to be determined by the Commission. However, Complaint Counsel disputes the veracity of the remaining assertions.

[29] The ALJ admitted RX644 subject to the following limitations and qualifications as to its evidentiary use: "(1) official notice is taken of the fact that the OGR investigated the activities of non-party witness Tiversa . . . and of the conclusions of the OGR staff as to the truthfulness and completeness of the information provided to the FTC by Tiversa and its president, Robert Boback; (2) statements purportedly made by Mr. Boback to the OGR, to the extent referred to in RX644, will not be considered for the truth of the matters asserted therein; and (3) documents provided to OGR, to the extent referred to in RX644 and not previously admitted into evidence in this case, will not be considered for the truth of the matters asserted therein." Order on Resp't's Mot. to Admit Exs. at 3 (July 15, 2015).

acknowledge that RX644 was excluded, much less argue that the ALJ erred in its ruling. The Commission should refrain from considering RX644, because the staff report could not be admitted for the truth of the matters asserted therein, as it constitutes an out-of-court statement relying upon multiple levels of out-of-court statements for the factual propositions and conclusions it sets forth.[30]

Respondent's baseless claims of collusion are unfounded and untrue, and they are unsupported by any evidence in the record. In any event, Complaint Counsel's precomplaint investigation is irrelevant to the disposition of this proceeding. As the ALJ noted, "[o]nce the Commission has . . . issued a complaint, the issue to be litigated is not the adequacy of the Commission's pre-complaint information or the diligence of its study of the materials in question but whether the alleged violation has in fact occurred." Order Granting in Part and Denying in Part Compl. Counsel's Mot. to Quash Subpoena on Compl. Counsel and for Prot. Order at 5-6 (Jan. 30, 2014) (citing *Exxon Corp.*, Docket No. 8934, 83 F.T.C. 1759, 1974 WL 175251, at *1-2 (1974)); *see also Boise Cascade Corp.*, Docket No. 9133, 97 F.T.C. 246, 1981 WL 389463, at *1 n.3 (Mar. 27, 1981) (holding that once a complaint issues, the Commission's determinations in issuing the complaint are reviewed "only in the most extraordinary circumstances"). In addition, to the extent Respondent is suggesting that Complaint Counsel's precomplaint investigation somehow taints this entire proceeding or violates LabMD's due process rights, Complaint

[30] Moreover, LabMD did not offer RX644 "for the truth of the matters set forth therein," Resp't's Mot. to Admit Select Exs. at 4-5 (June 12, 2015), and should not be permitted to do so now. Notwithstanding that RX644 is styled as a "Staff Report" and contains the conclusions of OGR staff, RX644 is not a public record for which FRE 803(8)'s hearsay exception applies, as it was prepared for the then-Chairman of OGR, and was not issued by the Committee, by vote or otherwise. *See* Fed. R. Evid. 803(8). Further, it does not fall under any other exception to the rule against hearsay. *See* Fed. R. Evid. 803. Nor does it bear satisfactory indicia of reliability to warrant admission under the Commission's Rules of Practice. *See* Rule 3.43(b); Compl. Counsel's Opp'n to Resp't's Mot. to Admit Select Exs. at 11-12 (June 24, 2015).

Counsel maintains that this position is incorrect as a matter of fact and law. *See supra* § VI.B at 35.

The Commission should likewise refrain from considering RX649 – a blog post written by a pseudonymous blogger with a blind quote purportedly from an "HHS spokesperson" – to which Respondent cites to support its argument that HHS chose not to join the FTC's case against LabMD because LabMD did not violate HIPAA or HITECH. RAB at 16-17. The ALJ excluded this evidence. Order on Resp't's Mot. to Admit Exs. at 2 (July 15, 2015). Again, Respondent does not acknowledge that such evidence was excluded, much less argue that the ALJ erred in his ruling. Regardless, the Commission should refrain from considering RX649, because it constitutes hearsay and hearsay within hearsay. *See* Compl. Counsel's Opp'n to Resp't's Mot. to Admit Select Exs. at 18 (June 24, 2015). RX649 does not fall within any exception to the rule against hearsay, *see* Fed. R. Evid. 803, and it does not otherwise bear satisfactory indicia of reliability, *see* Rule 3.43(b). In particular, the quotation from an "HHS spokesperson" that Respondent offers for the truth does not bear satisfactory indicia of reliability: it is not under oath, and the identity of the speaker is not provided.

## VII. THE PROPOSED ORDER IS NOT PUNITIVE

Respondent claims that the proposed order is punitive.[31] RAB at 24. As the Commission observed, however, "the complaint does not even seek to impose damages, let alone retrospective penalties." Comm'n Order Denying Resp't's Mot. to Dismiss at 17. The relief sought in the notice order – including the establishment of a comprehensive information security program, the requirement to prove breach notices to consumers, document retention, and compliance reporting – is appropriate and cannot be considered punitive. *See Riordan v. SEC*, 627 F.3d 1230, 1234-35 (D.C. Cir. 2010) (quoting *Drath v. FTC*, 239 F.2d 452, 454 (D.C. Cir. 1956)) (order preventing future misconduct is "purely remedial and preventative" and not a "penalty" or "forfeiture"). Likewise, the fencing-in relief of biennial assessments of LabMD's data security is necessary and appropriate, because LabMD's data security failings were serious, deliberate, and transferable. CCCL ¶¶ 91-103, 105-110, 112-114; *Telebrands Corp. v. FTC*, 457 F.3d 354, 362 (4th Cir. 2006); *Pom Wonderful LLC*, Docket No. 9344, Initial Decision at 314 (May 17, 2012).

[31] Any claim that LabMD has already been "punished" and driven out of business by the Commission's action is specious and is belied by the evidence and Michael Daugherty's own statements. In LabMD's suit in the Northern District of Georgia seeking a preliminary injunction and dismissal of this proceeding, the Court rejected this argument, because LabMD had remained very profitable for the majority of the investigation and had been denied insurance due to the administrative action only after LabMD had discontinued its cancer detection services. Slip Op., *LabMD, Inc. v. FTC*, No. 1:14-CV-00810-WSD, 2014 WL 1908716, at *6 n.8 (N.D. Ga. May 12, 2014) *aff'd*, 776 F.3d 1275 (11th Cir. 2015). In addition, Mr. Daugherty testified "that the implementation of the Affordable Care Act, and its resulting effect on cost containment and market consolidation negatively impacted LabMD's operations, and 'creat[ed] huge anxiety, destruction, consolidation in our customer base.'" *Id.* "Mr. Daugherty also conceded that LabMD's future 'depend[ed] on Obamacare, and other than that I don't know.'" *Id.*

## VIII. CONCLUSION

For the reasons set forth above and in Complaint Counsel's prior briefing, the Commission should grant Complaint Counsel's appeal and enter the proposed order attached to Complaint Counsel's Appeal Brief.

Dated: February 23, 2016

Respectfully submitted,

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

*Complaint Counsel*

## CERTIFICATE OF SERVICE

I hereby certify that on February 23, 2016, I caused the foregoing document to be filed electronically through the Office of the Secretary's FTC E-filing system, which will send notification of such filing to:

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

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

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, NW, Room H-110
Washington, DC 20580

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

Daniel Epstein
Patrick Massari
Erica Marshall
Alfred Lechner
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
daniel.epstein@causeofaction.org
patrick.massari@causeofaction.org
erica.marshall@causeofaction.org
jlechner@causeofaction.org
*Counsel for Respondent LabMD, Inc.*

## CERTIFICATE FOR ELECTRONIC FILING

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

February 23, 2016

By: _____
Jarad Brown
Federal Trade Commission
Bureau of Consumer Protection

# Attachment 1

*Docket:* **CIVIL ACTION No. 2015-1733-BLS 1**
*Date:* **November 19, 2015**
*Parties:* **KAMYRA WALKER and ANNE O'ROURKE, on behalf of themselves and a class vs. BOSTON MEDICAL CENTER CORP., MDF TRANSCRIPTION, LLC and RICHARD J. FAGAN**
*Judge:* **Edward P. Leibensperger**

MEMORANDUM AND ORDER ON DEFENDANTS' MOTION TO DISMISS

By letters dated April 23, 2014, or earlier, defendant, Boston Medical Center Corp. ("BMC"), notified plaintiffs and others similarly situated that their patient records from office visits with physicians "were inadvertently made accessible to the public through an independent medical record transcription service's online site." The letters noted that the medical records "could potentially be accessed by non authorized individuals" although BMC had "no reason to believe that this led to the misuse of any patient information." BMC could not say 'how long the information was publicly accessible through the site."[1]

Plaintiffs commenced this action on June 10, 2015. In their complaint, plaintiffs seek an injunction against further disclosure of their records and damages for the unauthorized exposure of their medical information to the public. They sue BMC, the medical record transcription servicer, MDF Transcription, LLC ("MDF"), and MDF's manager and owner, Richard J. Fagan. BMC and Fagan now move to dismiss the complaint.[2]

Plaintiffs do not know, at this stage, whether any unauthorized person actually gained access to their medical records. They allege, however, that "what goes on the internet, stays on the internet." They are fearful that their private information has been or will be disclosed to the public, a risk acknowledged by BMC's notice to them. They seek the opportunity to take discovery to learn the details regarding the length of time of the data breach, whether their records have been accessed and what steps have been taken to remedy the inadvertent disclosure. Their complaint contains seven counts: Count I, Invasion of Privacy under G.L. c. 214, ? 1B; Count II, Breach of Confidentiality; Count III, Breach of Fiduciary Duty; Count IV, Negligence; Count V, Negligent Supervision; Count VI, Breach of Implied Contract; and Count VII, Breach of Contract against MDF and Fagan. Plaintiffs claim that the breach by BMC and Fagan caused them injury. They seek an award of damages for that injury. In their breach of contract counts, plaintiffs also seek damages in the amount of a refund of amounts paid to BMC for medical services as a remedy for BMC's alleged breach.

BMC moves to dismiss pursuant to Mass. R. Civ. P. 12(b)(1) and 12(b)(6). The sum and substance of BMC's motion is that the complaint fails to allege any specific injury. In short, without an allegation that their medical records have actually been accessed by an unauthorized person or that their personal information is being utilized by an unauthorized person, plaintiffs lack standing and fail to state a claim.[3]

With respect to BMC's standing argument, I note the recent decision of the Supreme Judicial Court in Pugsley v. Police Department of Boston, 472 Mass. 367 (2015). There, the Court affirmed a dismissal for lack of standing upon a motion for summary judgment, not a motion to dismiss. Id. at 370. In doing so it articulated that an alleged injury must not be speculative, remote or indirect, but the Court also acknowledged that "real and immediate" risk of injury may be enough for standing. Id. at 371. Where, as here, plaintiffs allege facts that, if true, suggest a real risk of harm from the data breach at BMC, I conclude that the standing question should await a more full record and be decided upon a motion for summary judgment.[4]

With respect to a motion under Mass. R. Civ. P. 12(b)(6), it is required that the complaint set forth "factual 'allegations plausibly suggesting (not merely consistent with)' an entitlement to relief . . . ." Iannacchino v.

Ford Motor Co., 451 Mass. 623, 636 (2008), quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 557 (2007). The court must, however, accept as true the allegations of the complaint and draw every reasonable inference in favor of the plaintiff. Curtis v. Herb Chambers I 95, Inc., 458 Mass. 674, 676 (2011).

Applying that standard, plaintiffs' complaint adequately states a cognizable claim for relief. Support for that conclusion starts with drawing a reasonable inference from BMC's own letter informing plaintiffs of the data breach. From that letter it may be inferred that plaintiffs' medical records were available to the public on the internet for some period of time and that there is a serious risk of disclosure. It is reasonable to infer the next step that plaintiffs' records either were accessed or likely to be accessed by an unauthorized person. Plaintiffs are entitled to discovery to determine what access, if any, has occurred, among other things.

Plaintiffs general allegation of injury from the data breach, inferring, as I do, that there likely was or will be access to plaintiffs' confidential medical information by unauthorized persons, is sufficient. For example, a claim for an invasion of privacy involving disclosure of confidential medical records may give rise to damages for mental distress, harm to interest in privacy and special or economic harm. Restatement (Second) of Torts ? 652H (1977). Depending on the identity of a person who accessed the records, there could be financial damages. At the pleading stage, before discovery has determined whether plaintiffs' records were accessed, more specificity regarding the kind of injury suffered by plaintiffs is not required.

For the reasons stated above, BMC's motion to dismiss is DENIED. Fagan's motion to dismiss is also DENIED.

By the Court,

Edward P. Leibensperger
Justice of the Superior Court

[1] The letters are referenced in the complaint but not attached. In opposition to defendants' motion to dismiss, a copy of a letter was submitted by an affidavit of plaintiffs' counsel. BMC does not dispute the authenticity of the letter.

[2] According to the complaint, MDF was involuntarily dissolved in 2013. No responsive pleading has been served by MDF. Fagan appeared pro se by virtue of a letter to the court asking for dismissal. No cognizable grounds for dismissal were stated. Thus, Fagan's motion to dismiss is DENIED.

[3] In support of its motion, BMC submits the affidavit of its Chief Compliance Officer ("CCO"). Among other things, the CCO avers that "[t]here is no indication that any unauthorized third party gained access to Plaintiffs' medical records." Under the well established standards for ruling on a motion to dismiss, the court disregards the affidavit. Such factual statements are subject to discovery.

[4] BMC cites a number of federal cases addressing motions to dismiss for lack of standing in data breach cases. See, e.g., In re Horizon Healthcare Services Inc. Data Breach Litigation, 2015 WL 1472483 D. N. J. 2015). The Massachusetts standard for recognizing standing appears to be more liberal, allowing standing when there is risk of harm. How "real and immediate" the risk of harm is should be evaluated when the facts surrounding the data breach, including the quantity and nature of access to the records, are presented after discovery. See also, Tabata v. Charleston Area Medical Center, 233 W. Va. 512, 517 (Supreme Ct of Apps., W.Va. 2014)(standing recognized for claims about data breach even though there was no evidence of unauthorized access).